# User Manual

# Web Interface

# MC Technologies Router

# MC-MRL/MC-MRL-4
# MC-MRH/MC-MRH-4
# MC-MRE/MC-MRE-4

# Router Description

Mobile radio routers were designed for industrial use.
They allow switching as needed between mobile radio routers with high and medium bandwidth.

**Advantages at a glance:**

- Easy expansion of protected networks.
- High-security data transfer via IPsec or OpenVPN tunnel, plus integrated firewall.
- Easy and identical configuration of router family via integrated web server, USB stick or "remote".
- Compatible with mobile networks world-wide - can be used internationally.
- Event alerts by SMS and email.
- Top-hat rail mounting.
- Integrated logbook records device-specific events.
- Use of applications with RS232, RS485 or M-Bus interfaces on demand (only MC-MRL/MC-MRH/MC-MRE)
- Use of integrated GPS receiver for positioning on demand (only MC-MRH/MC-MRH-4).
- Delivered ready-to-use, including power supply plug, Ethernet connecting cable and mobile radio antenna.
- SIM cards are not included in the standard scope of delivery.

## Contents

**2. Additional functions**

# 1. 1. Configuration via the integrated web interface

## 1.1 Preparations

1. Hook the router up to the power supply using connection "P1" , "P2" or "POW".
2. To configure, connect the PC and the router to Ethernet port "ETH1" using an Ethernet cable.
3. For configuration, you will need a browser (i.e. Mozilla Firefox, Microsoft Internet Explorer, etc.) on a PC.
   The router must be connected to the power supply. The PC to be used for configuration must be connected to an Ethernet port on the router.

## 1.2 Configuration

### 1.2.1 Configuration via web interface

1. The PC must be set to "obtain IP address automatically".
   This is the default setting for PCs.
2. Open a browser on the PC.
3. Type the IP address (default: 192.168.0.1) in the address field.
4. For authentication purposes a user name and password must be entered. The default settings for the user name and password are both "admin", which should be entered in the corresponding fields. For your security, the password setting can be changed at any time using the "System/User" menu item on the web interface (see Page 39).

### 1.2.2 Local IP address is not (longer) known – configuration button

To reconfigure the router using the default IP address you will need to use the configuration button on the rear side of the device. This function depends on the setting you defined in Section 1.9.3 "Reset button".

**Web access reset**

The router is set to "Web access reset" unless you change the default setting. Press the configuration button for at least 5 seconds using a pointed object. The router web interface can be temporarily readdressed using the default IP address (192.168.0.1) for the Ethernet (LAN) connection. The configuration settings will not be lost when doing so.

**Important note!** The router does not supply any IP address to the connected PC via DHCP. You must thus assign a fixed IP address to the PC (e.g. 192.168.0.2, default gateway 192.168.0.1).

You will now have access to web management using the default access data. Please check the settings for the router IP address, user name and password and make any changes required.

**Factory reset**

You changed the setting to "Factory reset" (see Item 1.9.3 "System Configuration/Reset button"). Press the configuration button for at least 5 seconds using a pointed object. The router web interface can be readdressed using the default IP address (192.168.0.1) for the Ethernet (LAN) connection.

**Important note!** All configuration settings will be deleted and reset to the "Factory Defaults" setting.

### 1.2.3 Resetting all parameters on the web interface

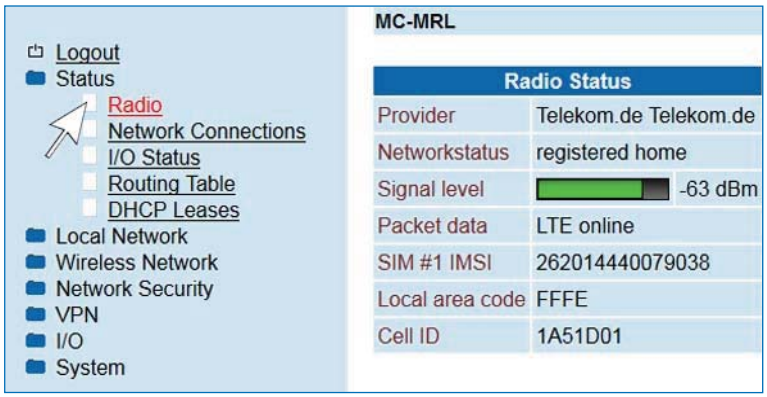
Resetting of all router settings to the factory default mode can be carried out via the internal web interface. Please click on the "Apply" button for the "Reset to Factory Defaults" function in the "System/Configuration Up-/Download" sub-menu.

# 1.3 Status

Display basic status information.

## 1.3.1 Radio

Display mobile connection.

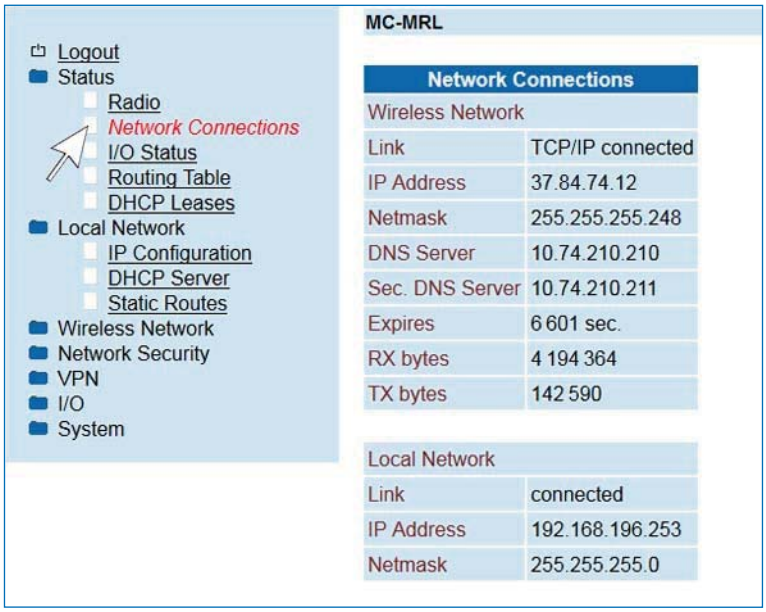



### Radio Status

| | | |
|---|---|---|
| Provider | Name of mobile service provider. | |
| Networkstatus | Status in cellular network. | |
| | Registered home: | Registered in the cellular network. |
| | Roaming: | Registered in a third-party cellular network. |
| | Waiting for PIN: | Waiting for PIN to be entered. |
| | Waiting for PUK: | Locked SIM card must be unlocked with PUK. |
| | Wrong PIN: | Wrong PIN configured in the router. |
| | No SIM Card: | Put SIM card in. |
| | Power off: | The GSM module is still off. |
| Signal level | Display receive level. | |
| Packet data | Offline: | No packet data connection. |
| | GPRS online: | Active GPRS connection. |
| | EDGE online: | Active EDGE connection. |
| | UMTS online: | Active UMTS connection. |
| | HSDPA/HSUPA online: | Active HSDPA/HSUPA connection. |
| | LTE online: | Active LTE connection. |
| SIM #1 IMSI | Specification of IMSI (International Mobile Subscriber Identity) by the SIM card. | |
| Local area code | Number in cellular network via current location. | |
| Cell ID | Clear recognition of a GSM cell in the cellular network. | |

## 1.3.2 Network Connections

Status information on mobile connection and on local Ethernet network.

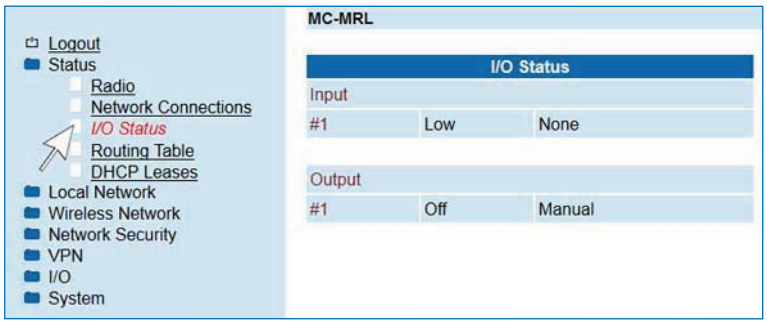



### Network Connections

| | | |
|---|---|---|
| **Wireless Network** | | |
| Link | TCP/IP connected: | Active GPRS/EDGE/UMTS/HSPA or LTE packet data connection in cellular network. |
| | VPN connected: | Active VPN connection via the cellular network. |
| | Not connected: | No packet data connection in the cellular network. |
| IP Address | Allocated IP address from the cellular network. | |
| Netmask | Allocated net mask from the cellular network. | |
| DNS Server | IP address of the DNS server. | |
| Sec. DNS Server | IP address of the alternate DNS server. | |
| Expires | Only MC-MRL (LTE) remainder duration until prompt for a new IP address. | |
| RX bytes | Sum of received data since last login to cellular network. | |
| TX bytes | Sum of sent data since last login to cellular network. | |
| **Local Network** | | |
| Link | Connected: | The local Ethernet is active. |
| | Not connected: | The local Ethernet is not active. |
| IP Address | Router IP address in the local network. | |
| Netmask | Router net mask in the local network. | |

## 1.3.3 I/O Status

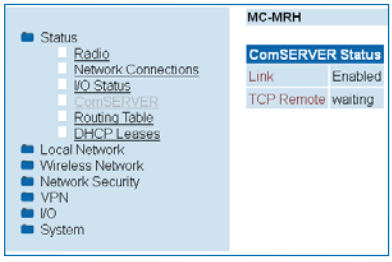
Status information of I/O interfaces IN and OUT.




| Input | Signal | Event |
|---|---|---|
| #1 | Low: The signal is low.<br>High: The signal is high. | None: No event has been triggered.<br>SMS: An SMS is being sent.<br>E-Mail: An email is being sent. |
| **Output** | **Signal** | **Event** |
| #1 | ON: Output active.<br>Off: Output is not active. | **Based on:** Manual ON, Remote Controlled ON, Radio Net work ON, Packet Service ON, VPN Service ON, Incoming Call ON or Connection lost ON. |

## 1.3.4 ComSERVER (only for MC Router with RS232 or RS485 interface on X1)

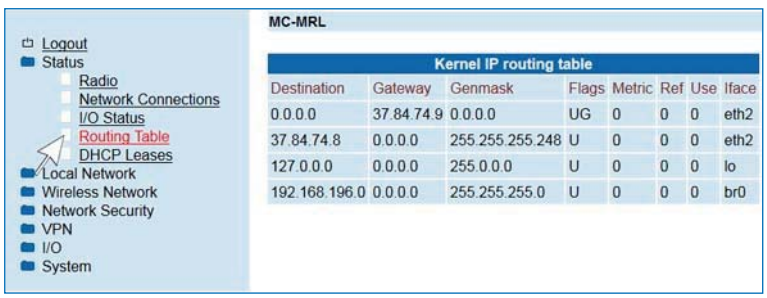
Status display of integrated ComSERVER




See also 1.9.6. ComSERVER

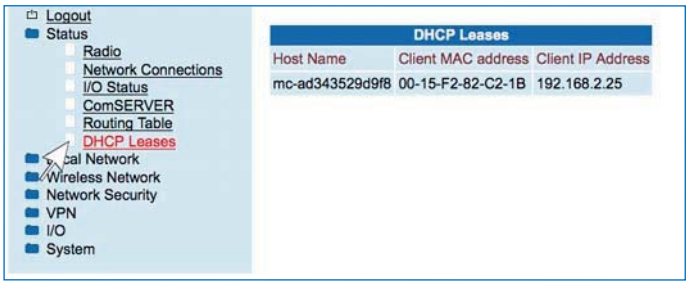
## 1.3.5 Routing Table

Display of current routing table.



### 1.3.6 DHCP Leases

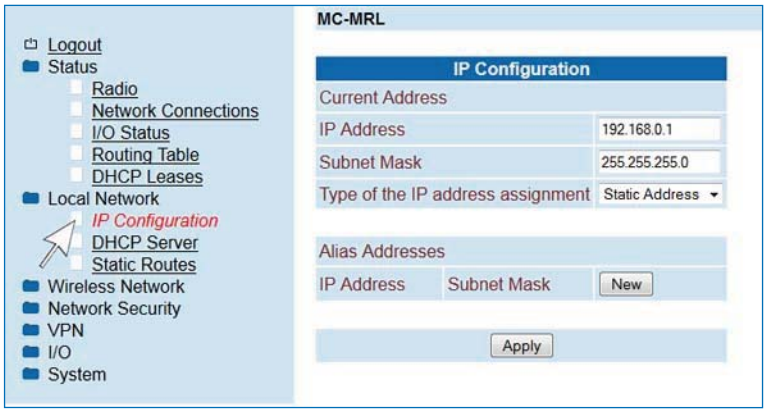
Display allocation of MAC address to IP address of terminal equipment connected to the local Ethernet. Connected terminal devices with a fixed IP address will not be shown.




## 1.4 Local Network

### 1.4.1 IP Configuration

Setup of local IP address and subnet mask for router. Set your parameters and click "Apply". Your parameters have been saved but not yet applied. To apply the setup, restart the router.

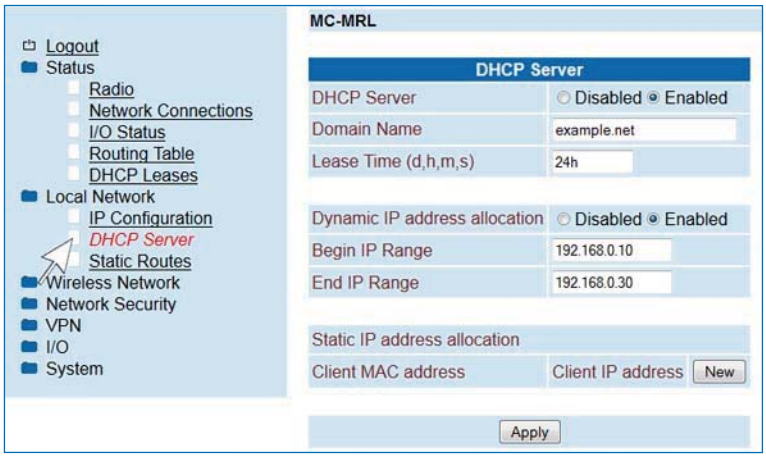



#### IP Configuration

| | | |
|---|---|---|
| **Current Address** | | |
| IP Address | Current local IP address of the router. If you forget the IP address and would like to configure the router, follow the instructions under 1.2 "Configuration" on Page 5. | |
| Subnet Mask | Current subnet mask. | |
| Type of IP address assignment | Static (default):<br>DHCP: | The IP address has been set.<br>The IP address and the subnet mask are obtained dynamically from a connected DHCP server. |
| **Alias Addresses** | | |
| IP Adress<br>Subnet Mask | Alias addresses how the router can be reached alternatively (up to eight other IP addresses).<br>Click "New" and add the other IP addresses, as well as the corresponding subnet masks. | |

## 1.4.2 DHCP Server

An IP address can be allocated automatically to local equipment connected via Ethernet using DHCP (Dynamic Host Configuration Protocol).

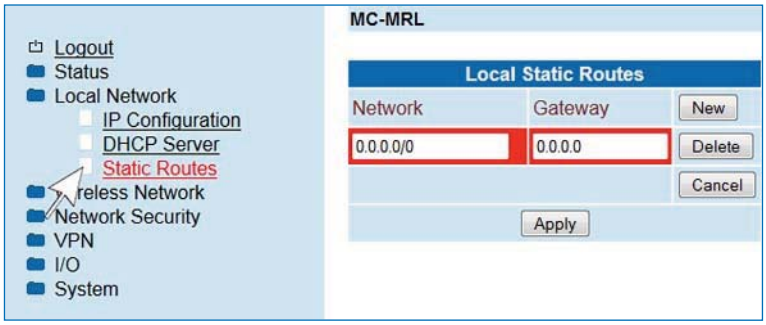



### DHCP Server

| | |
|---|---|
| DHCP Server | Disabled/Enabled: Click "Enabled" if the router should allocate the IP addresses to the connected terminal equipment as the DHCP server at start-up. |
| Domain Name | Domain name to be broadcast via DHCP. |
| Lease Time (d,h,m,s) | Validity period of allocated network configuration. |
| Dyn. IP address | Disabled/Enabled: Click "Enabled" if an IP address should be dynamically allocated to the connected terminal equipment in a set range. |
| Begin IP Range | Starting address for the address range from which IP addresses should be distributed. |
| End IP Range | Ending address for the address range from which IP addresses should be distributed. |
| Static IP address allocation | Static allocation of the IP address using the MAC address. |
| Client MAC address | MAC address of the terminal equipment. |
| Client IP address | IP address of the terminal equipment. Static allocation of the IP addresses should not overlap with the dynamic IP addresses. An identical IP address should not be used in multiple static allocations. |

## 1.4.3 Local Static Routes

Data packets from the local network can be defined by static routes using other gateways for alternative routes.



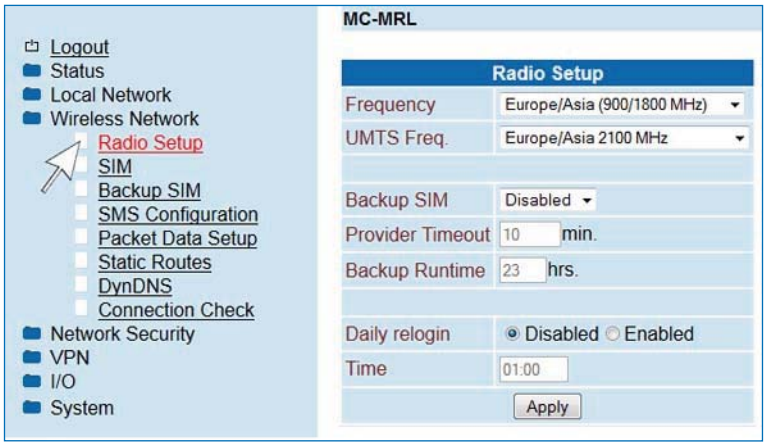

### Local Static Routes

| | |
|---|---|
| Network | Network in CIDR notation: IP address / Net mask<br>Example: xxx.xxx.xxx.xxx/yy (x..=IP address; yy=net mask)<br>Example: yy=24 (number of binary "ones") => net mask = 255.255.255.0 |
| Gateway | The gateway how this network can be reached. |

# 1.5 Wireless Network

Set-up for using the cellular network.

## 1.5.1 Radio Set-up

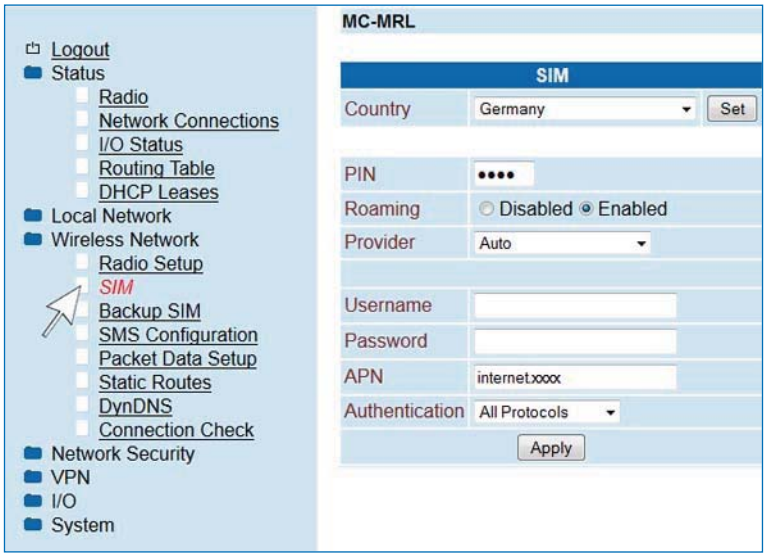



### Radio Set-up

| | | |
|---|---|---|
| Frequency | Set-up of the frequency range of the cellular network in which the router should work. | |
| UMTS Freq. | Set-up of the UMTS frequency range of the cellular network in which the router should work. | |
| | UMTS off: | Deactivate UMTS and HSPA. |
| Backup SIM (SIM2) | Disabled: | The back-up SIM (SIM2) is inactive. |
| | Enabled: | Back-up SIM active if a connection to the provider of the standard SIM (SIM1) for the set "provider timeout" period fails. The duration of the back-up SIM (SIM2) is determined by setting the "back-up runtime". After this period the standard SIM is reactivated. |
| | Always: | Only the back-up SIM (SIM2) is active. |
| | Input 1: | Switch to back-up SIM (SIM2) if input 1 high is on level. |
| Provider Timeout | Amount of time in minutes after which the back-up SIM card (SIM2) should be switched to if the primary cellular network (SIM1) is down. | |
| Backup Runtime | Amount of time in hours after which the primary cellular network (SIM1) should be switched back on. | |
| Daily relogin | Disabled: | Deactivate daily login. |
| | Enabled: | Activate daily login. Daily login first attempts to log onto primary cellular network (SIM1). |
| Time | Time of day at which the router independently logs out of the cellular network and logs back in. Relogin first attempts to log onto primary cellular network (SIM1). | |

## 1.5.2 SIM (SIM1)

Settings for the primary mobile connection via SIM1.

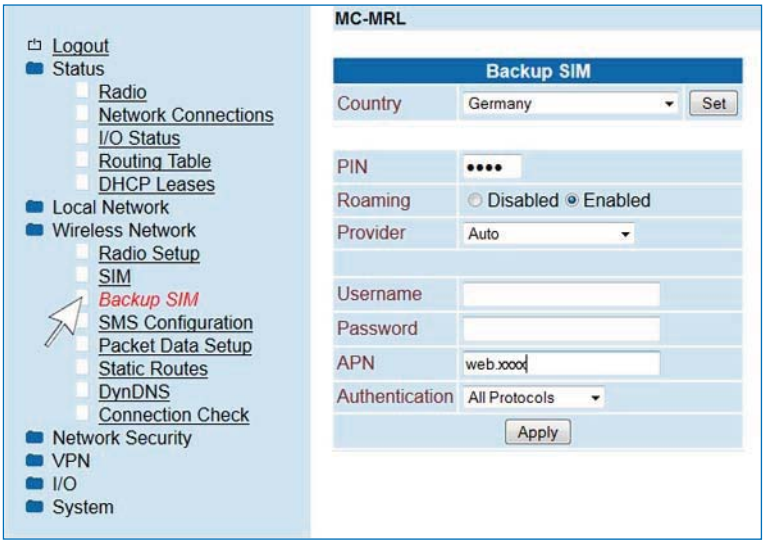



### SIM (SIM1)

| | |
|---|---|
| Country | Preselection of the country in which the router should operate. Under the menu option „Provider", you can then select the mobile service provider of the selected country. |
| PIN | PIN entry for SIM card SIM1. |
| Roaming | Set-up for use of third-party cellular networks.<br>Enabled: The router can log onto third-party networks. The "Auto" setting selects the provider with the strongest signal. This may result in additional cost, depending on the mobile service contract. Alternatively, you can choose a provider yourself.<br>Disabled: Roaming is deactivated and only the local network of the provider is used. If this network is not available, the router cannot connect to the Internet. |
| Provider | Selection of the provider via which the router connects to the Internet. The selection changes according to the country selected under "Country" in the menu.<br>Auto: The router selects the provider automatically. |
| Username | User name for access. |
| Password | Password for access.<br>The user name and the password are given to you by your mobile service provider. Do not leave the user name and password blank during configuration, even if the mobile service provider does not require any specific input! |
| APN | The APN is given to you by your mobile service provider. APN: (Access Point Name) is the name of the access point in the mobile service provider's packet data network. |
| Authentication | The default setting is "All protocols". Some providers require a specific authentication setting (refuse MSCHAP, CHAP only, PAP only) here. Consult your provider if necessary. |

## 1.5.3 Back-up SIM (SIM2)

Settings for the back-up mobile connection via SIM2.




### Back-up SIM (SIM2)

The same settings apply here as for Item 1.5.2 SIM (SIM1) (see Page 13).
The second SIM card (SIM2) is located inside the router housing. To insert or remove the SIM2 card, remove the back panel of the router.

## 1.5.4 SMS Configuration

### Controlling the mobile router by SMS

Under "SMS Control", click Enabled. Define an SMS password for security.
The password can comprise up to 7 alphanumeric characters.

### SMS Syntax

Commands are inputs using the following SMS syntax:

#<password>:<command>

| | | |
|---|---|---|
| <password> = ('A'-'Z', '0'-'9') | // | Up to 7 alphanumeric characters |
| <command> = SET:<sub_cmd> | // | Set command (ON) |
| <command> = CLR:<sub_cmd> | // | Clear command (OFF) |
| <sub_cmd> = OUTPUT | // | Output set to ON/OFF |
| <sub_cmd> = IPSEC | // | IPsec VPN 1 ON/OFF |
| <sub_cmd> = IPSEC:n | // | IPsec VPN n ON/OFF, n={1..x} |
| <command> = SEND:STATUS | // | Send a status SMS to the caller |
| <command> = RESET | // | Reset all alarms |
| <command> = REBOOT | // | Router reboot |

**Example:**

Turn on the I/O interface output. The (example) password is: "pw1212".
The SMS sent to the router's call number should then have the following content: #pw1212:SET:OUTPUT.

## Forwarding an SMS to a socket server

The router can forward received SMS messages to a terminal device through the Ethernet interface. A socket server must be installed on the terminal device to receive XML files.

Under "SMS forward", click Enabled. Enter the recipient's IP address and the port of the terminal device you want to talk to. The default value for the server is Port 1432. The received SMS is forwarded in the following example format:

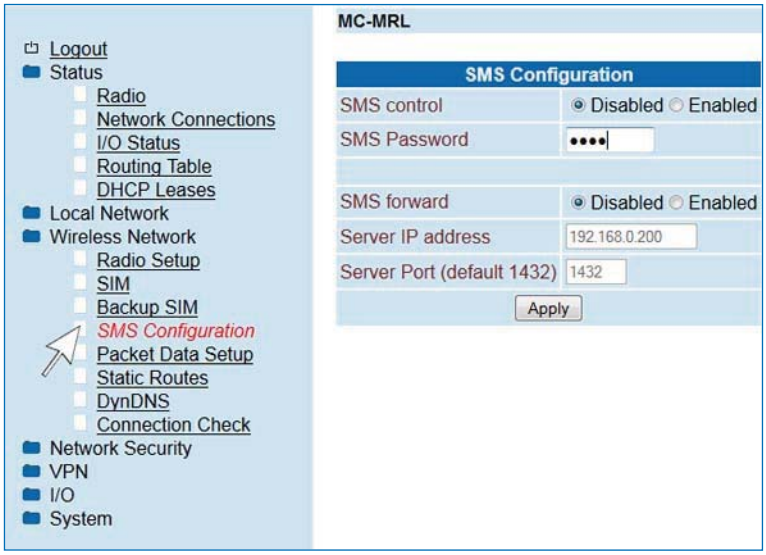
**Important note!**

The call number should be included as an entry in the phonebook (see Page 34) in order for the router to identify it.

**Example:**

```
<?xml version="1.0"?>
<cmgr origaddr="+49172123456789" timestamp="10/05/21,11:27:14+08">
SMS message</cmgr>
```

origaddr = Sender's call number
timestamp = Time-stamp of the Service Centre in GSM 03.40 format

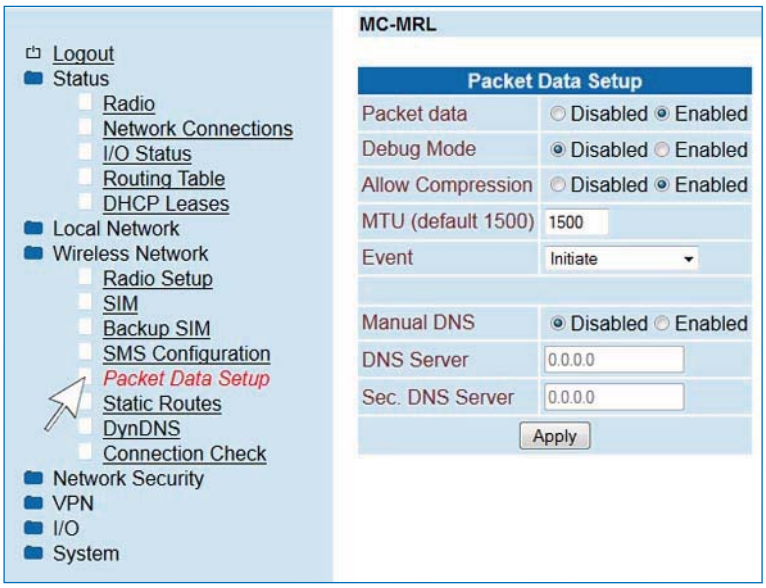



## SMS Configuration

| | |
|---|---|
| SMS control | Disabled: Remote control of router by SMS not possible.<br>Enabled: Remote control of router by SMS activated. |
| SMS Password | SMS password for remote control. |
| SMS forward | Disabled: Forwarding of SMS message via Ethernet not possible.<br>Enabled: Forwarding of SMS message via Ethernet activated. |
| Server IP address | IP address to which the SMS message should be forwarded. |
| Server Port (default 1432) | Port to which the SMS message should be forwarded. |

## 1.5.5 Packet Data Set-up

Activation and deactivation of the packet data connection via GPRS, EDGE, UMTS, HSPA or LTE.

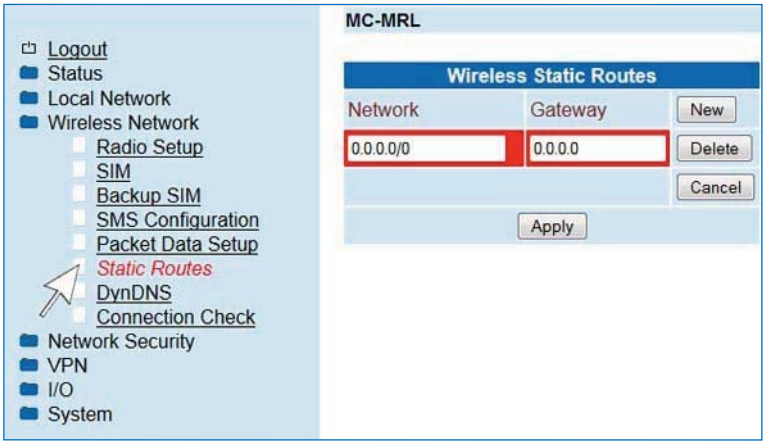



### Packet Data Set-up

| | |
|---|---|
| Packet data | Disabled: Access to GPRS/EDGE/UMTS/HSPA or LTE deactivated.<br>Enabled: Allow access to GPRS/EDGE/UMTS/HSPA or LTE. |
| Debug Mode | Disabled: Detailed information on packet data connection not saved in the log file.<br>Enabled: Detailed information on packet data connection saved in the log file. |
| Allow Compression | Disabled: Data compression of the packet data connection is deactivated.<br>Enabled: Data compression of the packet data connection is activated (default). |
| MTU (default 1500) | Maximum packet size in bytes in the packet data network. |
| Event | Definition of packet data connection start.<br>Initiate: Automatic start.<br>Initiate on Input #1: Start controlled through IN signal in the I/O interface. |
| Manual DNS | Disabled: Automatic DNS set-up. The DNS settings of the provider will be used.<br>Enabled: Manual DNS set-up. |
| DNS Server | IP address of the primary DNS server in the mobile service network. |
| Sec. DNS Server | IP address of the alternate DNS server in the mobile service network. |

## 1.5.6 Wireless Static Routes

Data packets from the local network can be defined using static routes for alternative routes in the mobile service network.



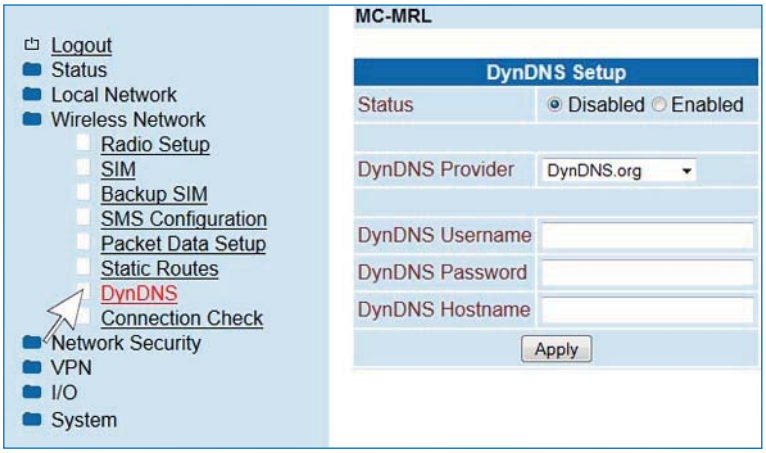

### Wireless Static Routes

| Wireless Static Routes | |
|---|---|
| Network | Network in CIDR notation. |
| Gateway | The gateway via which this network can be reached. |

## 1.5.7 DynDNS

The router IP address in the cellular network/Internet is allocated dynamically by the mobile service operator. A name can be allocated to the dynamic IP address using a DynDNS provider, via which the router can then be reached over the Internet. The DynDNS Client must be saved and activated in the router accordingly.

**Note:** For this to work, the provider must have allocated a public IP address to the router, not a private one. This is not the case with all providers. DynDNS cannot replace a static IP address and has limited reliability.



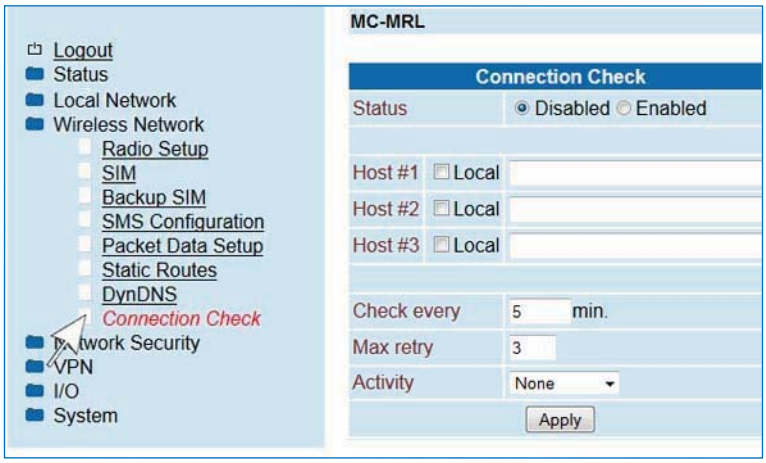

### DynDNS Set-up

| | |
|---|---|
| Status | Disabled: Deactivate DynDNS client.<br>Enabled: Activate DynDNS client. |
| DynDNS Provider | Select the name of the provider with whom you are registered, i.e. DynDNS.org, TZO.com, dhs.org., selfHost.de, custom DynDNS.<br>Use the "custom DynDNS" setting to select your preferred DynDNS provider. Please also enter the provider's server address under "DynDNS Server". |
| DynDNS Username | Enter the username for your DynDNS account here. |
| DynDNS Password | Enter the password for your DynDNS account here. |
| DynDNS Hostname | The host name selected for this router for DynDNS service. Your router can then be reached under this host name. |

## 1.5.8 Connection Check

For continuous connection monitoring, use "Connection Check" to check for a packet data connection in the mobile service network. If the connection is lost, an action can be configured for establishing a new connection.

**Note:** Please note that frequent connection checks can lead to increased data traffic and corresponding costs.




### Connection Check

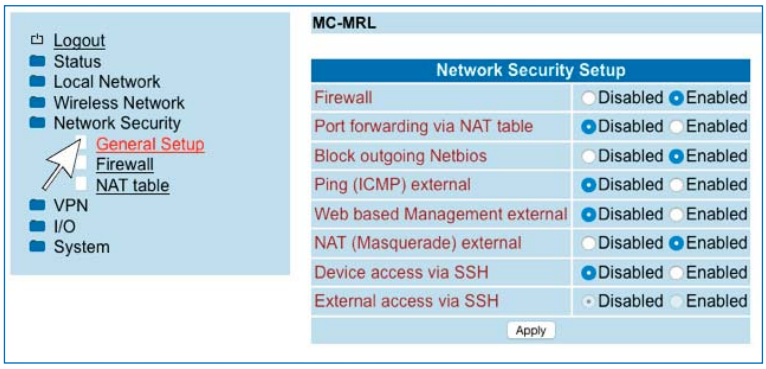
| | | |
|---|---|---|
| Status | Disabled: | Connection check is deactivated (default). |
| | Enabled: | Connection check is activated. |
| Host #1 ... #3 | IP address or host name of the reference point for the connection check.<br>"Local" option, when dealing with an address which can be reached via a VPN tunnel. | |
| Check every | Check interval in minutes. | |
| Max. retry | Number of repetitions until the configured action "Activity" is performed. | |
| Activity | Reboot: | Restart the router. |
| | Reconnect: | Re-establish packet data connection. |
| | Relogin: | Restart the cellular interface by redialing the mobile service network. |
| | None: | None. |

# 1.6 Network Security

## 1.6.1 General Set-up (Firmware 1.xx.x)

These settings apply for routers with 1.xx.x firmware (see Release Version under "System/Hardware").

**Important note!** Routers with Release 1.xx.x firmware cannot be updated to Version 2.xx.x. Please contact the manufacturer.



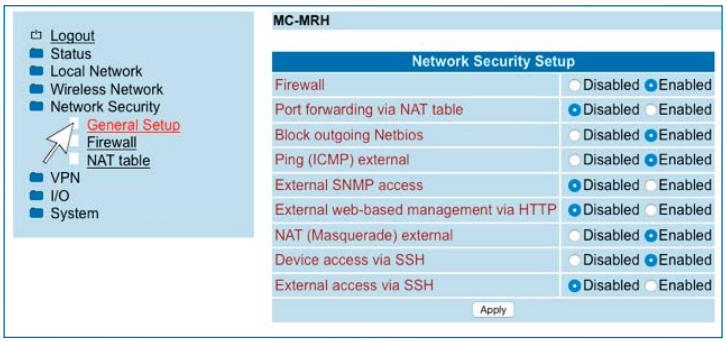
### General Set-up

| | |
|---|---|
| Firewall | Disabled: The integrated firewall is deactivated, no filtering of data packets.<br>Enabled: The integrated firewall is activated (default). |
| Port forwarding via NAT table | Disabled: Port forwarding via NAT table is blocked.<br>Enabled: Port forwarding via NAT table is allowed. |
| Block outgoing Netbios | Disabled: Outgoing NetBIOS requests are allowed.<br>Enabled: Outgoing NetBIOS requests are blocked (default). |
| Ping (ICMP) external | Disabled: A ping request from the external IP network to the router is ignored (default).<br>Enabled: A ping request from the external IP network to the router is returned. |
| Web based Management external | Disabled: External configuration via the web interface is not possible (default).<br>Enabled: External configuration via the web interface is possible. |
| NAT (Masquerade) external | Disabled: No IP masquerading performed.<br>Enabled: IP masquerading is activated. Communication from a private, local network to the Internet is allowed (default). |
| Device access via SSH | Disabled: Local SSH access to the router is not possible (default).<br>Enabled: Local SSH access to the router is possible. |
| External access via SSH | Disabled: Remote SSH access to the router is not possible (default).<br>Enabled: Remote SSH access to the router is possible. |

## 1.6.2 General Setup (Firmware 2.xx.x)

These settings apply for routers with 2.xx.x firmware (see Release Version under "System/Hardware").

**Important note!** Routers with Release 1.xx.x firmware cannot be updated to Version 2.xx.x. Please contact the manufacturer.



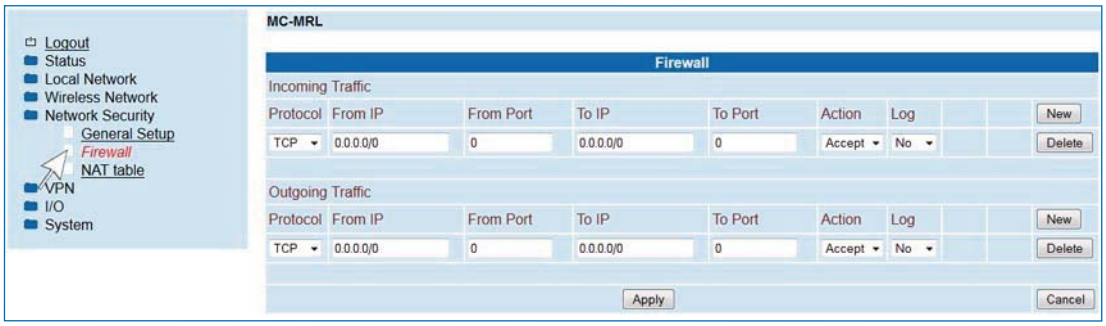

### General Set-up

| | |
|---|---|
| Firewall | Disabled: The integrated firewall is deactivated, no filtering of data packets.<br>Enabled: The integrated firewall is activated (default). |
| Port forwarding via NAT table | Disabled: Port forwarding via NAT table is blocked.<br>Enabled: Port forwarding via NAT table is allowed. |
| Block outgoing Netbios | Disabled: Outgoing NetBIOS requests are allowed.<br>Enabled: Outgoing NetBIOS requests are blocked (default). |
| Ping (ICMP) external | Disabled: A ping request from the external IP network to the router is ignored (default).<br>Enabled: A ping request from the external IP network to the router is returned. |
| External SNMP access | Disabled: Remote SNMP Access is not possible.<br>Enabled: Remote SNMP Access is possible. |
| External Web based Management via HTTP | Disabled: External configuration via the web interface is not possible (default).<br>Enabled: External configuration via the web interface is possible. |
| NAT (Masquerade) external | Disabled: No IP masquerading performed.<br>Enabled: IP masquerading is activated. Communication from a private, local network to the Internet is allowed (default). |
| Device access via SSH | Disabled: Local configuration via the web interface and https is not possible (default).<br>Enabled: Local configuration via the web interface and https is possible. |
| External access via SSH | Disabled: External configuration via the web interface and https is not possible (default).<br>Enabled: Configuration via the web interface and https is possible. |

## 1.6.3 Firewall

The MCT router includes a Stateful Packet Inspection Firewall.
The firewall can be turned on or off (see "Network Security Setup," menu point "Firewall.") The firewall is active by default and blocks incoming data traffic. Outgoing data traffic is still possible.

The firewall rules are applied from up to down.

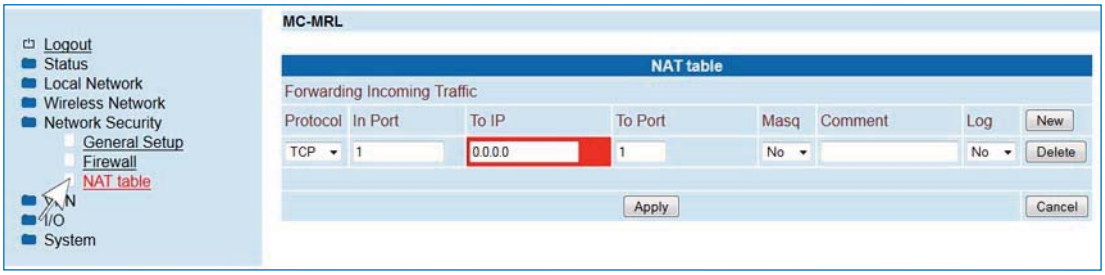



### Firewall

| | | |
|---|---|---|
| **Incoming Traffic** | | |
| Protocol | TCP, UDP, ICMP, all | |
| From IP<br>To IP | 0.0.0.0/0 means all IP addresses. To enter an address range, use CIDR notation. | |
| From Port<br>To Port | (only with TCP and UDP) You have the following options: | |
| | 1. Direct port input | Example: From Port = 20, To Port = 30. |
| | 2. Any | Examples: From Port or To Port = Any (Any means absolutely any port). |
| | 3. Port range | Example: From Port or To Port = 80-90 (all ports from 80-90). |
| Action | Accept: | Pass data packets. |
| | Reject: | Data packets are rejected. |
| | Drop: | Data packets may not pass, the sender does not receive notification. |
| Log | Logging firewall rules. | |
| | Yes: | Event is logged. |
| | No: | Event is not logged (default). |
| New | A new firewall rule is added below the last rule. | |
| | Delete: | The rule is deleted. |
| **Outgoing Traffic** | Lists the installed firewall regulations. They apply for outgoing data connections that were internally initiated to communicate with a remote destination device.<br>Factory settings: The factory settings include a rule allowing all outgoing connections.<br>**Note:** If no rule is set, all outgoing connections are blocked (except VPN). | |
| Protocol | TCP, UDP, ICMP, all | |
| From IP | 0.0.0.0/0 means all IP addresses. To enter an address range, use CIDR notation. | |
| From Port<br>To Port | (Only evaluated for TCP and UDP logs.) You have the following options: | |
| | 1. Direct port input | Example: From Port = 20, To Port = 30. |
| | 2. Any | Examples: From Port or To Port = Any (Any means absolutely any port). |
| | 3. Port range | Example: From Port or To Port = 80-90 (all ports from 80-90). |
| Action | Accept: | Pass data packets. |
| | Reject: | Data packets are rejected. |
| | Drop: | Data packets may not pass, the sender does not receive notification.Logging of firewall rules. |
| | Yes: | Event is logged. |
| | No: | Event is not logged (default). |
| New | A new firewall rule is added below the last rule. | |
| | Delete: | The rule is deleted. |

## 1.6.4 NAT table (port forwarding)

Rules for NAT (Network Address Translation).
The router has only one IP address, via which it can be accessed externally.
Data packets can be redirected to internal IP address ports via additional transmitted port numbers.




### NAT table

| | |
|---|---|
| Protocol | TCP, UDP, ICMP |
| In Port<br>To Port | (only with TCP and UDP) You have the following options:<br>1. Direct port input Example: In Port = 20, To Port = 30.<br>2. Port range Example: In Port = 80-90 To Port = 100-110. |
| To IP | 0.0.0.0/0 means all IP addresses. To enter an address range, use CIDR notation. |
| Masq | For every individual rule, you can determine if IP masquerading should be applied.<br>Yes: IP masquerading is activated, reply to cellular network is possible.<br>No: (Default) reply to cellular network is not possible. |
| Comment | Entering a comment. |
| Log | Logging firewall rules.<br>Yes: Event is logged.<br>No: Event is not logged (default). |
| New | The "New" button allows a new rule to be added under the last rule.<br>The "Delete" button deletes the rule from the table. |

**Note:** After clicking "Apply", perform a reboot (see Page 44) or restart the router (interrupt the power supply).

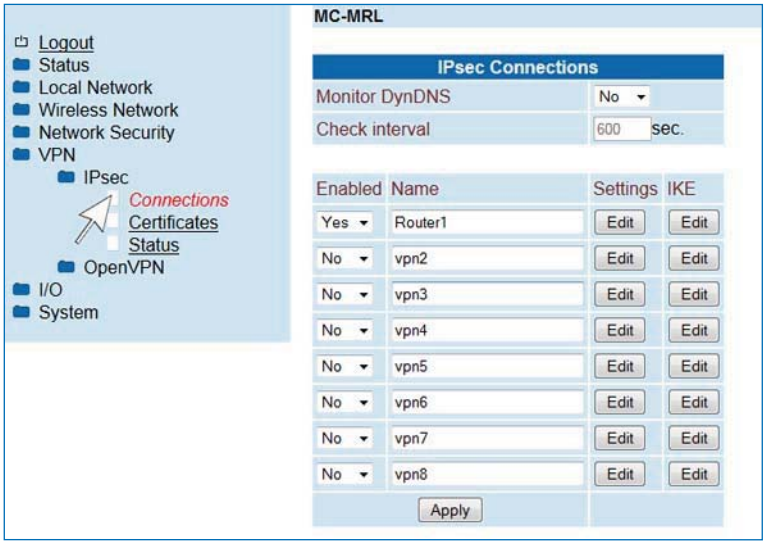
# 1.7 VPN

## 1.7.1 IPsec

### 1.7.1.1 Connections

IPsec (Internet Protocol Security) is a security protocol used for communicating over IP networks.

For a VPN connection, the IP addresses of the VPN remote peers must be known and addressable.
The VPN remote peer must support IPsec with the following configuration:
– Authentication by X.509 certificates or Preshared Secret Key (PSK)
– ESP
– Diffie-Hellman Group 2 or 5
– 3DES or AES encryption
– MD5 or SHA-1 hash algorithms
– Tunnel mode
– Quick mode
– Main mode
– SA lifetime (1 second to 24 hours)

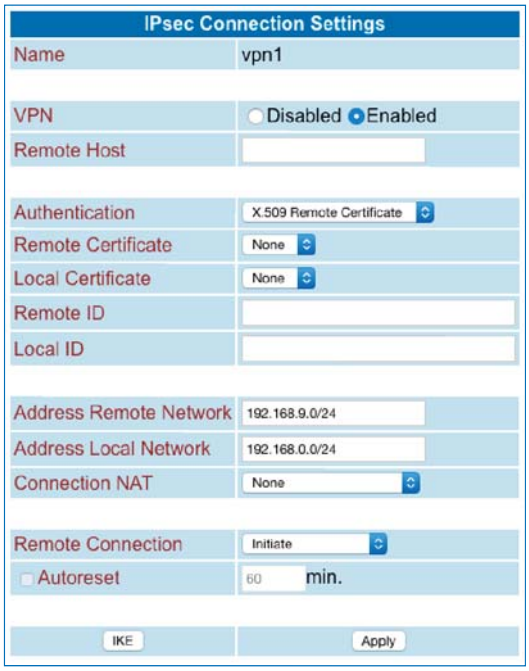



**IPsec Connections**

| | |
|---|---|
| Monitor DynDNS | If DynDNS is used as "Remote Host", the "Monitor DynDNS" function should be set to "Yes". |
| Check interval | Check interval in seconds. |
| Enabled | Activate or deactivate VPN connection. |
| Name | Arbitrary name of VPN connection. |
| Settings | VPN connection settings. |
| IKE | The "Edit" menu includes settings to establish IKE (Internet Key Exchange protocol) automatic key management for IPsec (see Page 25). |

## IPsec Connection Settings > Edit


Remote Connection "Accept"




Remote Connection "Initiate ..."

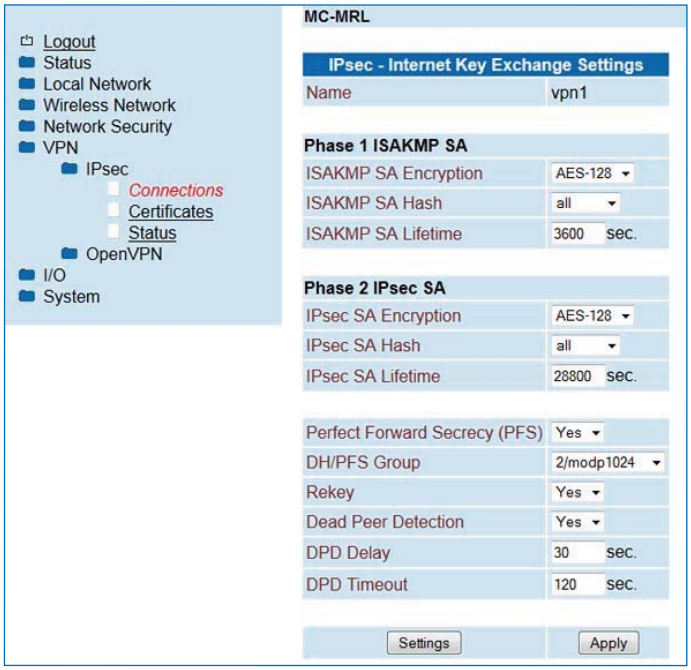
### IPsec Connection Settings

| | | |
|---|---|---|
| Name | Name of the VPN connection. | |
| VPN | Active = Enabled, Inactive = Disabled. | |
| Authentication | X.509 Remote Certificate: | Each VPN participant has a private, secret key as well as a public key in the form of a X.509 certificate which contains further information about its owner and a certification authority (CA). |
| | Preshared Secred Key (PSK): | Each VPN participant knows a shared password. |
| | X.509 Remote + CAuth: | Like an X.509 certificate but with entry of the user name and password (e.g. when using Shrew Soft as a VPN client). |
| Remote Certificate | VPN remote peer certificate. The certificate must be loaded ahead of time. | |
| Local Certificate | Local certificate with which the router identifies itself to the VPN remote peer (machine certificate, PKCS#12.) The certificate must be loaded ahead of time. | |
| Remote ID | If the field is left empty (default,) the information from the certificate is used.<br>Name for identification by remote peer. This must correspond to the information from the router certificate. | |
| Local ID | If the field is left empty (default,) the information from the certificate is used.<br>The local ID allows you to set the name with which the router identifies itself to the remote peer.<br>For more details, see Remote ID. | |
| Virtual Remote Address | Virtual remote IP address when using clients that cannot connect networks<br>(e.g. PC with Shrew Soft VPN software, smartphones, etc.). | |
| Address Remote Network | IP address/subnet mask of the remote network to which the VPN connection needs to be established. | |

### IPsec Connection Settings

| | |
|---|---|
| Address Local Network | IP address/subnet mask of the local network. |
| Connection NAT | None: No NAT on other IP addresses.<br>Local 1:1 –NAT -> NAT to local Network: 1 to 1 NAT on the local network. Setting of the start IP address. |
| Remote Connection | Direction of connection establishment:<br>Accept: Wait for the remote peer to establish the connection.<br>Initiate: The router establishes the connection.<br>Initiate on SMS: Connection established after reception of valid SMS.<br>Initiate on Call: Connection established after valid call.<br>Iniatiate on Input: Connection established after switch signal on IN of the I/O interface. |
| Autoreset | Click here and set a time in minutes after which the connection should be automatically disconnected. |

## IPsec Connection IKE > Edit




### IPsec Connection IKE

| | |
|---|---|
| IPsec - Internet Key Exchange Settings | Name of the VPN connection. |
| **Phase 1 ISAKMP SA** | |
| ISAKMP SA Encryption | AES-128 (default). AES-192, AES-256, 3 DES. |
| ISAKMP SA Hash | The setting "all" accepts either MD5 or SHA-1. |
| ISAKMP SA Lifetime | Life cycle of a key in seconds (3600 = 1 hour). |

### IPsec Connection IKE

| | |
|---|---|
| **Phase 2 IPsec SA** | Unlike Phase 1 ISAKMP SA (key exchange,) this is where the procedure for **Data exchange** is determined. It can differ from the key exchange procedure. |
| IPsec SA Encryption | AES-128 (default). AES-192, AES-256, 3 DES. |
| IPsec SA Hash | The setting "all" accepts either MD5 or SHA-1. |
| IPsec SA Lifetime | Life cycle in seconds for the key specified for IPsec SA.<br>28800 seconds = 8 hours (default).<br>86400 seconds = 24 hours (maximum). |
| Perfect Forward Secrecy (PFS) | Yes: Perfect Forward Secrecy activated.<br>No: Perfect Forward Secrecy deactivated. |
| DH/PFS Group | Key exchange procedure (Diffie-Hellman groups for Internet Key Exchange (IKE)).<br>5/modp1536 = High encryption.<br>2/modp1024 = Normal encryption (default). |
| Rekey | Yes: A new key will be brokered.<br>No: No new key will be brokered. |
| Dead Peer Detection | Recognition of validity and resulting action in case of interruption of IPsec connection.<br>Yes: Dead Peer Detection activated (i.e. Restart at VPN Initiate).<br>No: No Dead Peer Detection. |
| DPD Delay | Time interval to next check. |
| DPD Timeout | Time period after which the connection to the remote peer should be declared inactive.<br>Default value: 120 seconds.<br>Maximum: 86400 seconds (24 hours). |

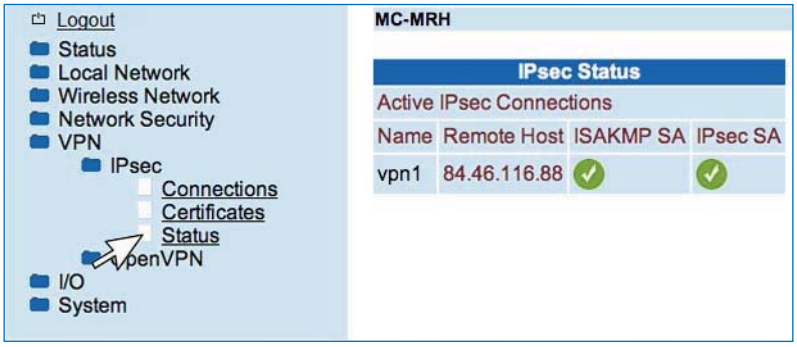
## 1.7.1.2 Certificates

The router authenticates itself to the remote peer with a certificate that can be uploaded onto the router.
By clicking "Apply", you upload the certificate onto the router.

### Certificates

| | | |
|---|---|---|
| Load Remote Certificate | Upload | - Upload the remote peer certificate (.cer .crt).<br>Under VPN > IPsec > Connections > Settings > Edit, you assign the certificate for the VPN connection. |
| Load Own PKCS#12 Certificate | Upload | - Upload the certificate (in PKCS#12 format, xxx.p12) to be used for the local router.<br>Under VPN > IPsec > Connections > Settings > Edit, you assign the certificate to the VPN connection. |
| | Password | - Enter the password given during exporting. |
| Remote Certificates | | List of imported .cer /.crt certificates. |
| | Delete | - Delete a certificate. |
| Own Certificates | | List of imported PKCS#12 certificates |
| | Delete | - Delete a certificate. |

## 1.7.1.3 Status



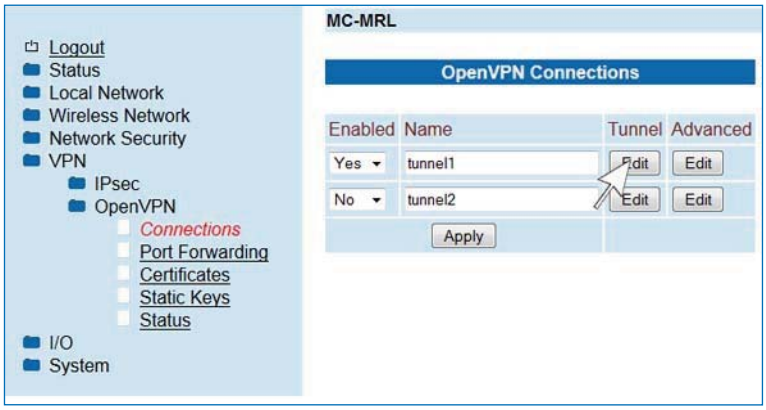

### IPsec Status

| | |
|---|---|
| Active IPsec Connections | An active VPN connection is indicated by a green symbol. |

## 1.7.2 OpenVPN
## 1.7.2.1 Connections (Tunnel 1 and 2)

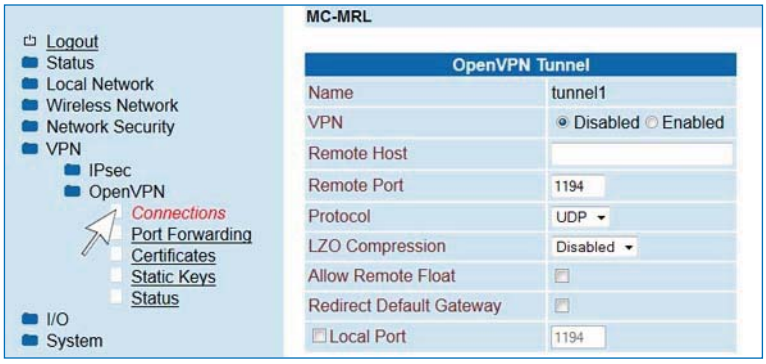
OpenVPN establishment of a virtual private network (VPN) via an encrypted connection.
Two OpenVPN tunnels can be set up at the same time (Tunnel 1 and Tunnel 2.)
The configuration of Tunnel 1 and Tunnel 2 is identical.

**OpenVPN Connections**




Select an OpenVPN connection and click "Edit".

**OpenVPN Tunnel**

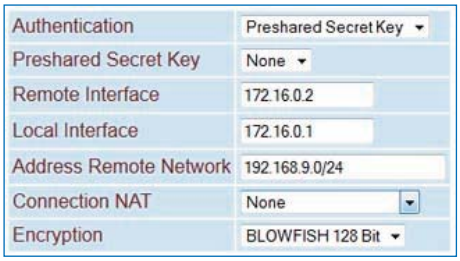



| | |
|---|---|
| Name | Arbitrary name of OpenVPN connection. |
| VPN | Enabled: OpenVPN Tunnel activated.<br>Disabled: OpenVPN Tunnel deactivated. |
| Remote Host | IP address or URL of the remote peer to which the tunnel will be established. |
| Remote Port | Port of the remote peer to which the tunnel will be established (default 1194). |
| Protocol | Protocol selection (UDP or TCP). |
| LZO Compression | Disabled: Switched off or not allowed.<br>Adaptive: (Data) adaptive compression switched on.<br>Yes: Switched on but can be switched off from the server.<br>No: Switched off but can be switched on from the server.<br>Enabled: Compression allowed; type of compression determined by the server. |
| Allow Remote Float | Activate this option to accept authenticated packets from each IP address during OpenVPN connection. This option is recommended if IP addresses are used for dynamic communication. |
| Redirect Default Gateway | The default gateway is directed via the tunnel. |
| Local Port | Determines a fixed port for the OpenVPN client. |

## OpenVPN Tunnel X.509 Certificate


| | |
|---|---|
| Authentication | X.509 Certificate - Authentication procedure for X.509 certificate. |
| Local Certificate | Ascertains which certificate the router will use to identify itself to the VPN remote peer. |
| TLS Authentication Key | Selection of a static key for an additional TLS Auth signature. The same key must then be used on the other side. The static key must have been generated and/or uploaded in advance under VPN > OpenVPN > Static Key. |
| Check Remote Certificate Type | Activate this option to check the OpenVPN connection certificates. |
| Connection NAT | None: No forwarding.<br>Local 1:1 NAT: "One-to-one" forwarding to a local network (NAT to local network).<br>Local Masquerding: The packets going out through the tunnel are rewritten to the router source address so that equipment on the router can access the other side of the tunnel.<br>Port Forwarding: Forwarding with the setting described under 1.7.2.2.<br>Host Forwarding: Forwarding to the fixed IP address of a connected terminal device (Forward to local Host). |
| Encryption | Encryption algorithm for the OpenVPN connection. |

## OpenVPN Tunnel Preshared Secret Key

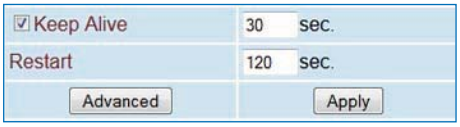



| | |
|---|---|
| Authentication | Preshared Secret Key – authentication procedure with a static key (Preshared Key). |
| Preshared Secret Key | Ascertains preshared secret key the router uses to identify itself to the VPN remote peer. |
| Remote Interface Certificate Type | Virtual, remote IP address of the remote peer certificate type. |
| Local Interface | Virtual local IP address of the router. |
| Address Remote Network | Address range of the remote network. |
| Connection NAT | None: No forwarding.<br>Local 1:1 NAT: "One-to-one" forwarding to a local network (NAT to local network).<br>Local Masquerding: The packets going out through the tunnel are rewritten to the source address of the router to allow equipment on the router access to the other side of the tunnel.<br>Port Forwarding: Forwarding with the setting described under 1.7.2.2.<br>Host Forwarding: Forwarding to the fixed IP address of a connected terminal device (Forward to local Host). |
| Encryption | Encryption algorithm for the OpenVPN connection. |

### OpenVPN Tunnel User name/Password


| | |
|---|---|
| Authentication | Username/Password - Set-up of user name and password. |
| CA Certificate | Enter the OpenVPN server CA certificate. |
| Check Remote Certificate Type | Specifying whether the remote certificate should be evaluated. |
| Username | Enter user name. |
| Password | Ente password. |
| Connection NAT | None: No forwarding.<br>Local 1:1 NAT: "One-to-one" forwarding to a local network (NAT to local network).<br>Local Masquerading: The packets going out through the tunnel are rewritten to the router source address so that equipment on the router can access the other side of the tunnel.<br>Remote Masquerading: The packets coming in through the tunnel are rewritten on the local router address.<br>Port Forwarding: Forwarding with the setting described under 1.7.2.2.<br>Host Forwarding: Forwarding to the fixed IP address of a connected terminal device (Forward to local Host). |
| Encryption | Encryption algorithm for the OpenVPN connection. |

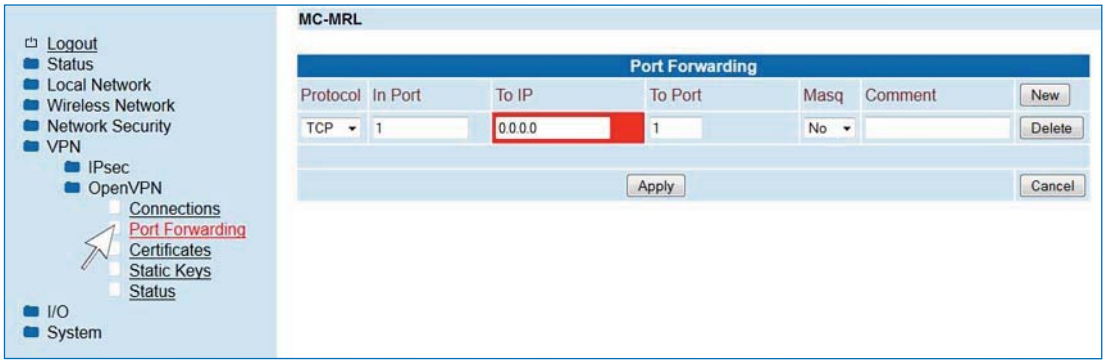
### Keep Alive




| | |
|---|---|
| Keep Alive | Time period in seconds after which Keep Alive requests should be sent. These requests test whether the remote peer is still available.<br>Default setting: 30 seconds. |
| Restart | Time period in seconds after which the connection to the remote peer should be restarted if there is no reply to the Keep Alive requests.<br>Default setting: 120 seconds. |

## 1.7.2.2 Port Forwording

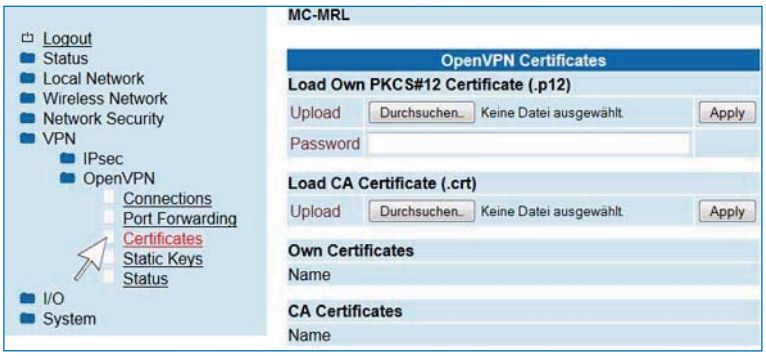
Rules for Port Forwarding: The router has only one IP address via which it can be accessed externally. Data packets can be redirected to internal IP address ports via additional transmitted port numbers.




| | |
|---|---|
| Protocol | TCP, UDP, ICMP |
| In Port / To Port | (TCP and UDP only) You have the following options:<br>To Port 1. direct port input - Example: In Port = 20, To Port = 30.<br>2. Port range - Example: In Port = 80-90 To Port = 100-110. |
| To IP | Input of a target IP address, 0.0.0.0/0 means all IP addresses. |
| Masq | For every individual rule, you can determine if IP masquerading should be applied.<br>Yes: IP masquerading is activated, reply to VPN tunnel is possible.<br>No: (Default) reply to VPN tunnel is not possible. |
| Comment | Input comment. |

## 1.7.2.3 Certificates

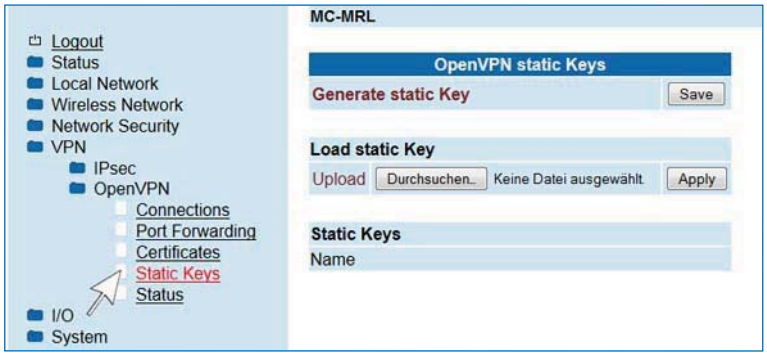
Certificate for authentication of the router to the remote peer.



### Certificates

| | | |
|---|---|---|
| Load Own PKCS#12 | Upload | Upload the certificate (in PKCS#12 format, xxx.p12) to be used for the local router. Under VPN > OpenVPN > Client, you can assign one of these certificates to each VPN connection under Local Certificate. |
| | Password | Password with which the PKCS#12 file is protected during export. |
| Load CA certificate (.crt) | Upload | Upload the CA certificate. |
| Own Certificate | Name | Display the uploaded certificates and keys. |
| CA Certificate | Name | Display the uploaded CA certificates and keys. |

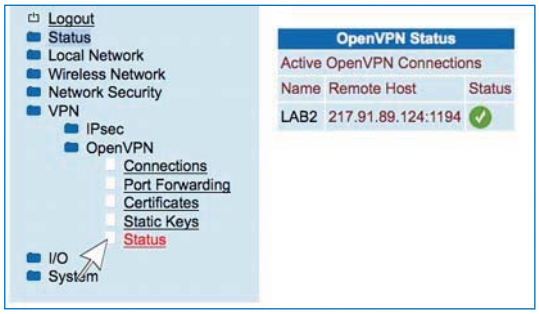
## 1.7.2.4 Static Keys (Preshared Key)




### Static Keys

| | |
|---|---|
| Generate static Key | Click on "Save" to generate and save a static key file. |
| Load static Key | Upload: Upload the static key file. The same file must be uploaded to the remote peer's OpenVPN server. |
| Static Keys | List of uploaded static key files. |

## 1.7.2.5 Status




### OpenVPN Status

| | |
|---|---|
| Active OpenVPN Connections | Status of the active VPN connection. |

# 1.8 I/O

The router has an I/O input and output (Input/Output).
The router **input** behaves as follows:

**Input Low:** An input voltage of less than 5-6 volts is recognized as a Low signal.
**Input High:** An input voltage over 5-6 volts is recognized as a High signal. The maximum input voltage is 30V. Input current is limited to max. 4mA.

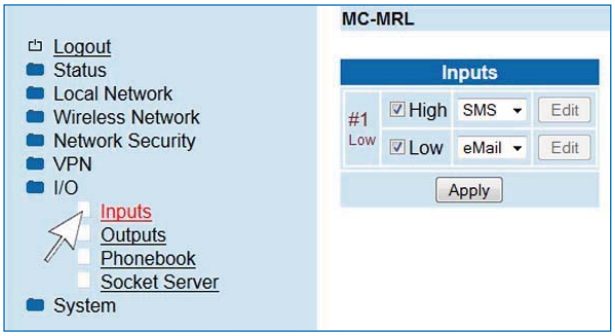
The physical behaviour of the router output is as follows:

**Output Low:** The output is highly resistant.
**Output High**: The operating voltage (10-30V) minus approx. 0.5V is switched to the outside. Its maximum load is 180 mA, following which the current limiter will be activated and the voltage will drop.

Example: If the router is operated using 24V, the "Output High" at the output will be approx. 23.5V.
In the case of "Output Low" there will be 0V at the output.

## 1.8.1 Inputs

The switch input can be used to send SMSs or email. Please check to see if the switch input is already being used to start a VPN connection. If so, it will not be possible to use it to send SMS or emails.



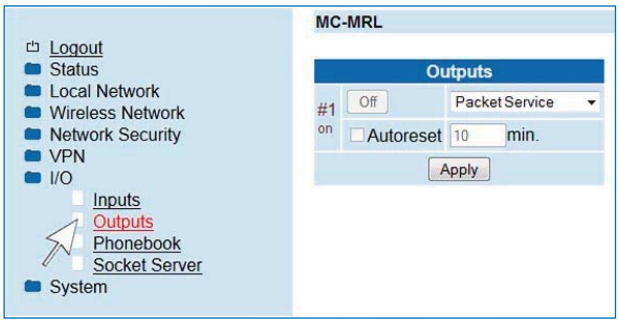

### Inputs

| | |
|---|---|
| High | When activated, an SMS or email will be sent when there is a "High" level at the switch input. Select the type of message and click "Apply". Then click "Edit". For SMS, select the corresponding phonebook entry and enter your message under "Message Text". For an email alert, fill out the email form. |
| Low | When activated, an SMS or email will be sent when there is a "Low" level at the switch input. Select the type of message and click "Apply". Then click "Edit". For SMS, select the corresponding phonebook entry and enter your message under "Message Text". For an email alert, fill out the email form. |

**Note:** To send an email, the email account under the section 1.9.8 (see Page 40-41) SMTP Configuration must be set up.

## 1.8.2 Outputs

The router switch output can be controlled remotely or switched using a router connection status.

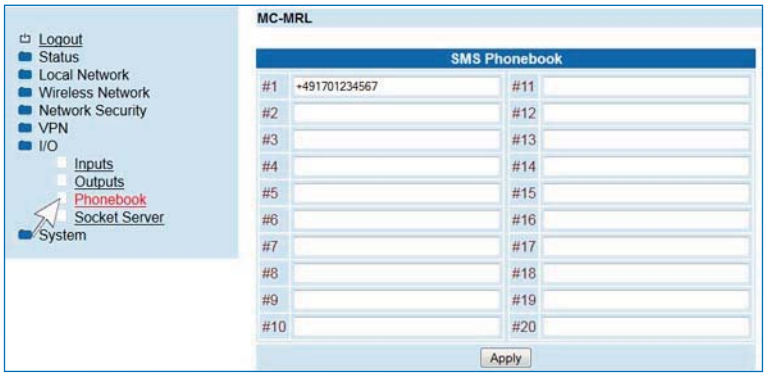


**Outputs**

| | | |
|---|---|---|
| Functions | Manual: | Switch the output by clicking ON or OFF in the web interface. |
| | Remote Controlled: | Switch the switch output remotely by SMS (see Page 13) or by Control command to the socket server (see page 14). |
| | Radio Network: | The switch output is active when the router is registered in a mobile service network. |
| | Paket Service: | The switch output is active when the router has established a packet data connection and received a valid IP address from the provider. |
| | VPN Service: | The switch output is active when the router has established a VPN connection. |
| | Incoming Call: | The switch output is active when the router is called from a call number entered in the phonebook (Caller ID). |
| | Connection Lost: | The switch output is active when the router connection check does not reach the configured address. |
| | Timer: | Reserved for timer functions. |
| Autoreset | "Autoreset" resets the switch output after the preset period of time. | |

## 1.8.3 Phonebook

List of the call numbers for receivers of the SMS messages, as well as for authentication (Caller Id) for authorization to switch the switch outputs.




## 1.8.4 Socket Server

The router includes an integrated socket server and can be made to perform the following actions by receiving XML files:

1. Set and query I/O signals
2. Send messages such as email and SMS
3. Query the router status

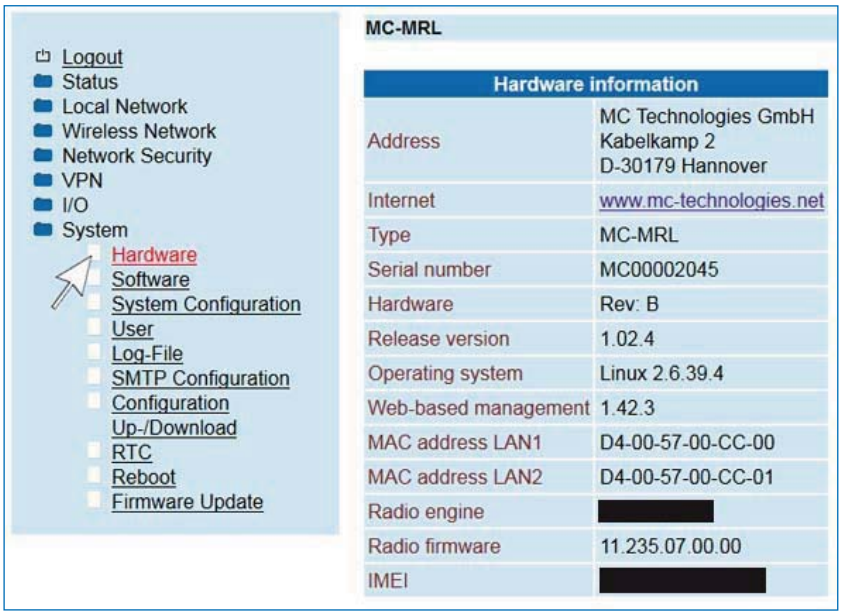
To use these functions, the socket server must be set to "Enabled" in the socket configuration. The socket server port can be configured as desired, the default setting is Port 1432.

For examples of sending and receiving I/O status, email, SMS and router status using XML files via the router socket server see Section 2.2.1 (Page 47).

# 1.9 System

This section provides information on the hardware, software and status of the router.

## 1.9.1 Hardware

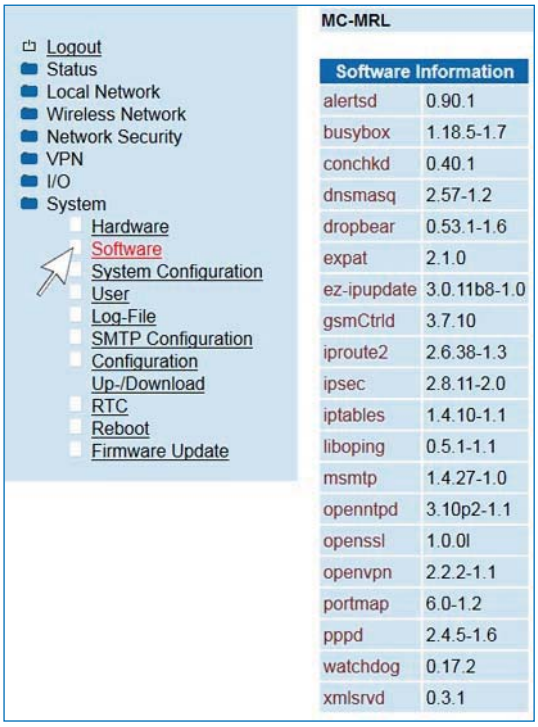



### Hardware Information

| | |
|---|---|
| Address | Address of the manufacturer. |
| Internet | Internet address of the manufacturer. |
| Type | Article description of the router. |
| Serial number | Serial number of the router. |
| Hardware | Hardware version of router. |
| Release version | Release version of router software. |
| Operating system | Version of operating system. |
| Web-based management | Version of web interface. |
| MAC address LAN1 | MAC address of Ethernet Connection 1. |
| MAC address LAN2 | MAC address of Ethernet Connection 2. |
| Radio engine | Type of cellular module used. |
| Radio firmware | Firmware version of the cellular module. |
| IMEI | The IMEI (International Mobile Station Equipment Identity) is a 15-digit serial number which can be used to accurately identify every cellular module. |

## 1.9.2 Software

This menu item lists all the software modules installed, including their versions.



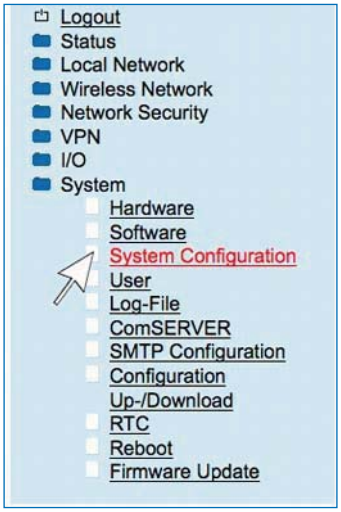

## 1.9.3 System Configuration

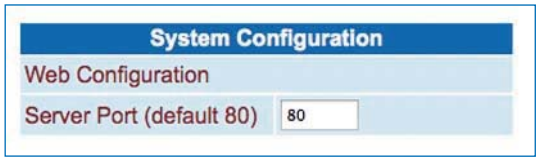
### Web Configuration

The router web interface can normally be reached via the browser without additionally indicating a port or by additionally indicating Port 80. The port can be changed here if needed.

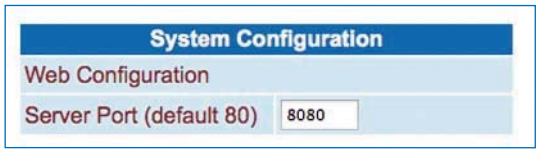
Example using router address 192.168.0.1:

Web interface address: 192.168.0.1 or 192.168.0.1:80




After changing the port to, for instance,
8080 address of the web interface: 192.168.0.1:8080

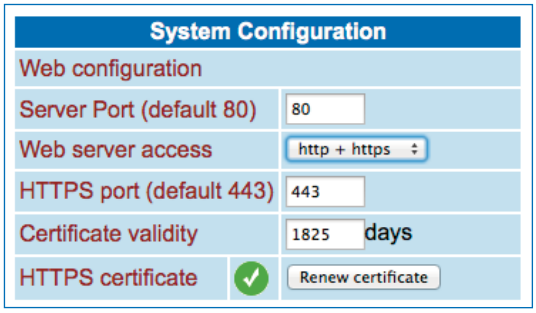



**Note:** After clicking "Apply", perform a reboot (Page 44) or restart the router (interrupt the power supply).

## Web server access

The router web interface can be accessed via http or https (secure) and/or http + https.

**Important note!** This function is only supported by 4-port routers (MC xx-4) or 2 port routers (MC xx) with firmware beginning with 2.xx.x (See: "System / Hardware / Release" e.g. 2.04.2).

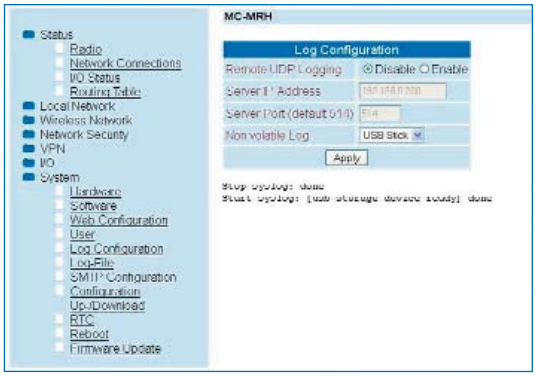



### Web server access

| | | |
|---|---|---|
| Web server access | http: | http access only. |
| | http + https: | http and https access. |
| | https: | https access only. |
| HTTPS port (default443) | Alter the https default port here. | |
| Certificate validity | Validity of the https certificate in days. | |
| HTTPS certificate | Renew certificate: | Local generation of an https certificate. Click again to renew the certificate. |

## Log Configuration

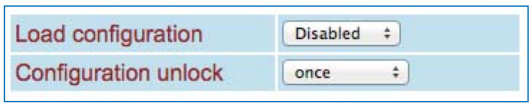
Log files can be saved on an external log server via UDP.




### Log Configuration

| | | |
|---|---|---|
| Remote UPD Logging | Disabled: | No logging on external server. |
| | Enabled: | Logging on external server. |
| Server IP address | Server IP address. | |
| Server Port (default 514) | Server port. | |
| Non volatile Log | Disabled: | Logging on the internal RAM. |
| | USB stick: | Logging on the USB stick on the front plate. |
| | SD card: | Logging on internal SD card. The SD card is not included in the scope of delivery. |

## Load Configuration



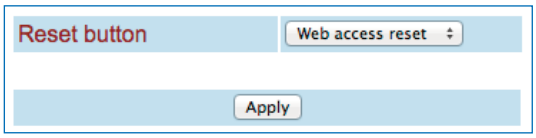

### Load configuration

| | | |
|---|---|---|
| Load Configuration | Disabled: | Uploading of the configuration from a USB stick or internal SD card is deactivated. |
| | USB stick: | A configuration from a USB connected to the router has been uploaded. |
| | SD card: | A configuration from the internal SD card has been uploaded. |
| | | If the upload was successful, the setting is automatically set to "Disabled". The setting must be reconfigured to USB stick or SD card for a new upload. |
| | | **Note:** The internal SD card slot is accessible by removing the back cover. |
| Configuration unlock | once: | The configuration is only uploaded once from the storage medium (USB stick or SD card). |
| | always: | The configuration is always uploaded from the storage medium (USB stick or SD card) after the router is booted. |
| | by Input 1: | The configuration is uploaded from the storage medium (USB stick or SD card) when there is a High signal from the input (I/O). |

Click "Apply" to save your configuration.

## Reset button

To reconfigure the router using the default IP address or to set the configuration to the factory default settings you will need to use the configuration button on the rear side of the device (See Item 1.2.2). The following settings allow you to define which function should be permanently assigned to the configuration button.



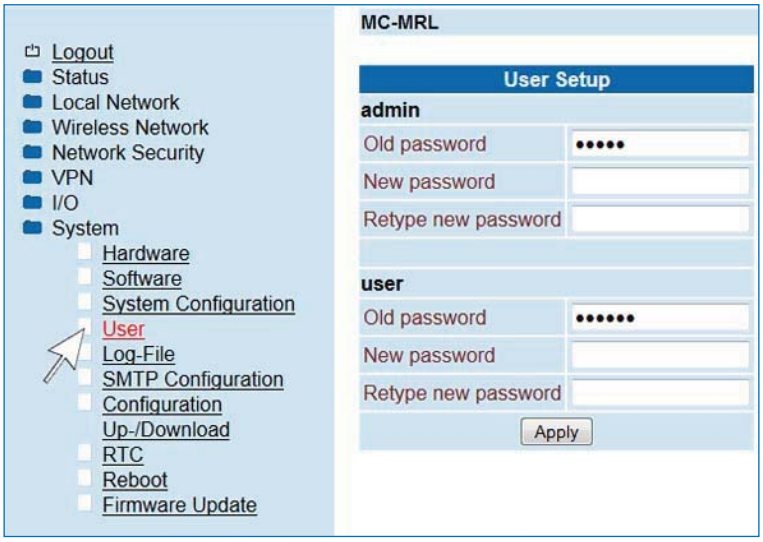


### Reset button

| | | |
|---|---|---|
| Reset button | Web access reset: | Press the reset button to readdress the router web interface using the default IP address (192.168.0.1) for the Ethernet (LAN) connection. The configuration settings will not be lost when doing so. |
| | Factory reset: | Press the reset button to readdress the router web interface using the default IP address (192.168.0.1) for the Ethernet (LAN) connection. All configuration settings will be deleted and reset to "Factory Default". |

Click "Apply" to save your configuration.

## 1.9.4 User

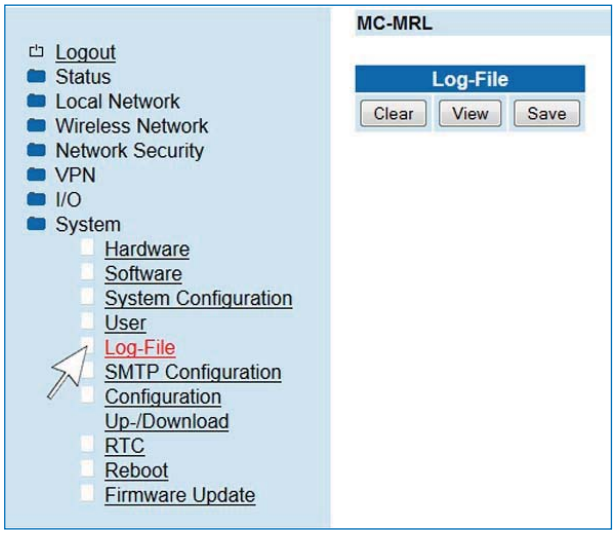



**User Set-up**

| | |
|---|---|
| admin | Access to all areas - password modification (default: admin). |
| user | Only access - password modification (default: public). |

## 1.9.5 Log File

All router activities are indicated in a log file. When the maximum storage capacity is reached, the oldest entries are overwritten.




**Log File**

| | |
|---|---|
| Clear | All entries are deleted. |
| View | Log file display. |
| Save | Storage of the log file as a text file on a user PC. |

## 1.9.6 ComSERVER (Only for MC Router with RS232 or RS485 interface on X1)

For remote access to terminal equipment with a serial interface, a virtual COM port connection can additionally be established over long distances as a standard router function.

MC Technologies MC-MRL, MC-MRH and MC-MRE routers are optionally equipped with an RS232 or RS485 interface at X1 for this purpose. For detailed information, please refer to the MC Technologies Application Note 41 Router (COM-Port connection via MC router - RS232/RS485).


| | |
|---|---|
| Status | Disabled: The ComServer is deactivated.<br>Enabled: The ComServer is activated. |
| Connection Type | Server RAW - Usage without RFC 2217 Client Server Protocol.<br>Server RFC 2217 - Usage with RFC 2217 Client Server Protocol. |
| Server Port (default 3001) | Set the TCP port via which the ComServer is to be addressed. |
| Flow control | Set flow control:<br>RFC 2217 - With an RS232 application<br>RS485 RTS - With an RS485 application |

**Note:** RFC 2217 is a Standard Client Server Protocol used as a standard protocol when using multiple device servers (ComServer.) The RFC 2217 protocol allows for the use of various "COM port redirector" softwares for virtual Com Port Interfaces on the PC.

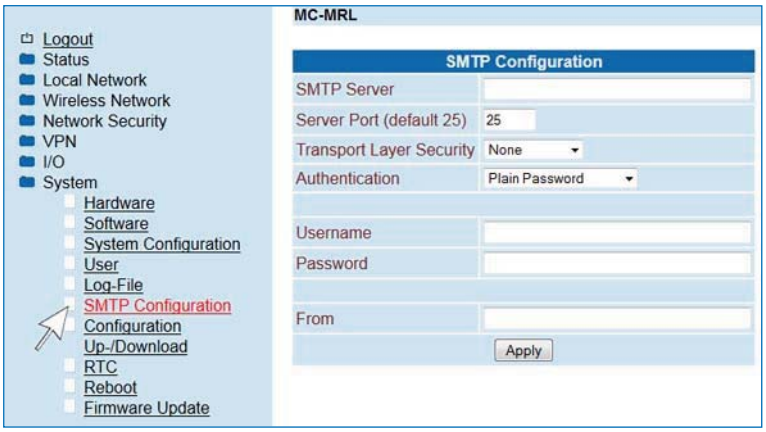
## 1.9.7 SMTP configuration

### SNMP Configuration

| | |
|---|---|
| **System information** | |
| Name of Device | For example: Device name. |
| Description | Short description. |
| Physical location | For example: name of the location. |
| Contact | For example: The admin's email address. |
| **SNMPv1/v2 Community** | |
| Enable SNMPv1/v2 access | Yes: SNMP is supported.<br>No: SNMP is not supported. |
| Read Only | Password for read only access. |
| Read and write | Password for read and write access. |
| **Trap Configuration** | |
| Trap Manager IP address | Enter the recipient's IP address. |
| Port | Port (Default 162). |
| Target Community | Recipient's password. |
| Sending traps | Disabled: No traps are sent.<br>Enabled: Traps are sent. |

## 1.9.8 SMTP configuration - sending emails

To send emails as described under 1.8.1 Input (page 33), an email server must be configured with the support of the SMTP protocol. Please use your selected email account's access data.

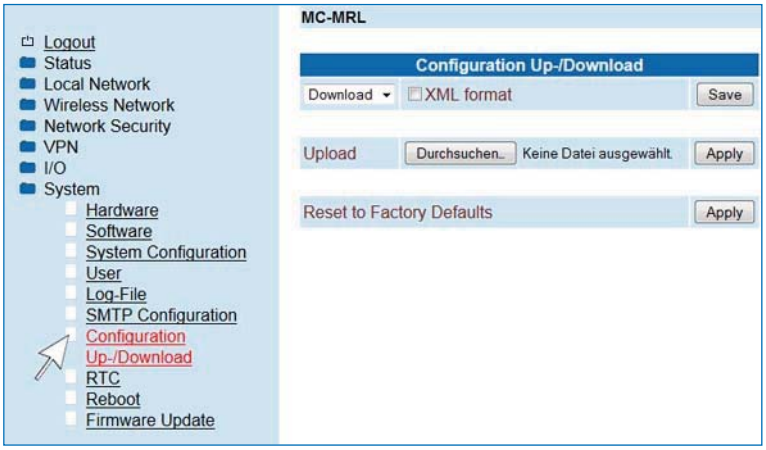



### SMTP Configuration

| | |
|---|---|
| SMTP Server | Host name or mail server IP address. |
| Server Port (default 25) | Mail server port. |
| Transport Layer Security | None: Unencrypted connection to the mail server.<br>STARTTLS: After STARTTLS encrypted connection to the mail server.<br>SSL/TLS: Encrypted connection to the mail server via SSL/TLS. |
| Authentication | No authentication: No authentication required.<br>Plain Password: Authentication using user name and password.<br>Encrypted Password: Authentication using user name and password plus encrypted transmission. |
| Username | User name for logging onto the mail server. |
| Password | Password for logging onto the mail server. |
| From | Sender's email address. |

## 1.9.9 Configuration Up-/Download

The configuration can be stored as a CFG file (default) or as an XML file on the user PC. Configurations stored on this PC can be uploaded to the router.

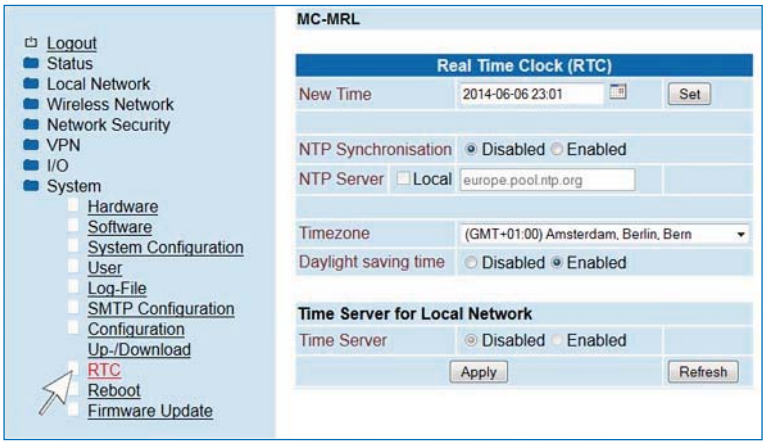



### Configuration Up-/Download

| | | |
|---|---|---|
| Download | Download: | Store the current configuration in a file on a connected PC. |
| | USB stick: | Store the current configuration in a file on a USB stick inserted into the router. |
| | SD card: | Store the current configuration in a file on the internally inserted SD card (The SD card slot can be accessed by opening the rear housing panel). |
| XML format | Check this box to save the configuration in XML format. | |
| Upload | Upload a stored configuration. | |
| Reset to Factory Defaults | The configuration is set to factory default settings.<br>VPN certificates stored in the router are not affected. | |

**Note:** Configuration using SSH and XML file.
The transfer of an XML file for router configuration can also be carried out using the SSH protocol via the local Ethernet interface or in remote operation. Please follow the description under 2.1 (Page 45).

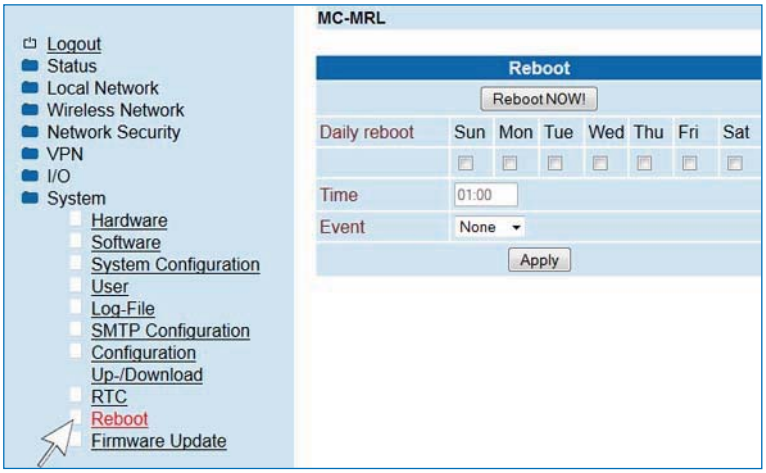
## 1.9.10 RTC - Setting the time and date / Time Server




### Real Time Clock (RTC)

| | |
|---|---|
| New Time | Manually set the time when no time server (NTP server) is available. |
| NTP Synchronisation | Disabled: No NTP synchronisation.<br>Enabled: The router obtains date and time from a time server. |
| NTP Server | Local: Use a local NTP server.<br>NTP - Network Time Protocol - The router can be used as an NTP server for a terminal device connected to "ETH1" or "ETH2". The terminal device must then use the router address as an NTP server. NTP synchronization must be set to "Enabled". |
| Timezone | Timezone selection. |
| Daylight saving time | Disabled: Without daylight saving time.<br>Enabled: With daylight saving time. |
| **Time Server for Local Network** | |
| Time Server | Enabled: The router is operated as a time server in the local network.<br>Disabled: The router is not a time server for the local network. |

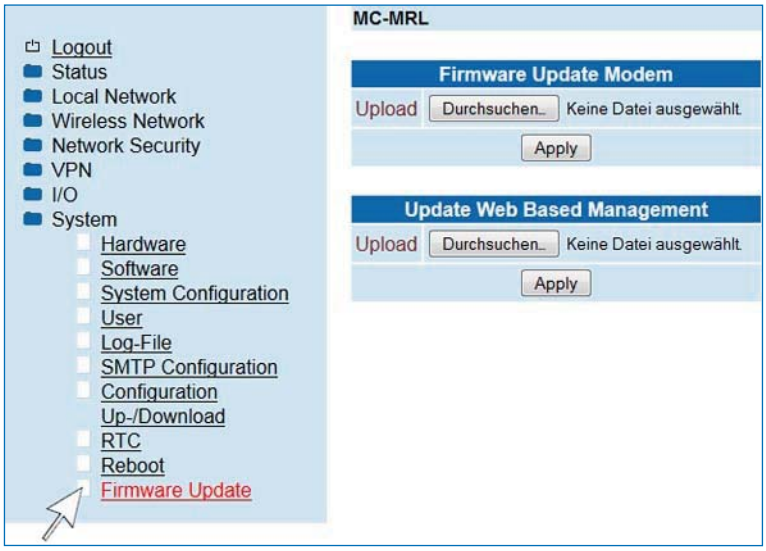
## 1.9.11 Reboot - restarting the router




**Reboot**

| | |
|---|---|
| Reboot NOW! | Router immediately shut down and then restarted. |
| Daily reboot | Set the day of the week for a reboot. |
| Time | Enter time of reboot in the format: Hour: Minute. |
| Event | Input1: A restart can be triggered via a HIGH signal to the switching input I/O IN. Please ensure that the switching input is ultimately set back to LOW to prevent another restart.<br>None: No event for a reboot. |

## 1.9.12 Firmware Update




| | |
|---|---|
| Firmware Update Modem | Upload: Upload the latest firmware to the router. |
| Update Web Based Management | Upload: Upload the latest web interface to the router.<br>Not required as standard because the web interface is included in the firmware and will also be revised when an update is issued. |

# 2. 2. Additional functions

## 2.1 Router configuration using SSH and XML file

The router can be configured using the SSH protocol via the local Ethernet interface or in remote operation.

SSH or Secure Shell refers to both a network protocol and a corresponding programme which allows an encrypted network connection to be generated using a remote device.

In **Linux**, use console input. In **Windows**, we recommend using the programs **plink.exe** and **pscp.exe**, which can be downloaded at putty.org.

The examples below are based on the router default settings:

**Username:** **admin**
**Password:** **admin**
**Router IP-Address:** **192.168.0.1**

### 2.1.1 Download configuration via SSH

You can download the router configuration as an XML file or as a TGZ file.

**For Linux:**

*ssh admin@192.168.0.1 'su -c "/usr/sbin/export_cfg"' > config.xml*

oder

*ssh admin@192.168.0.1 'su -c "/usr/sbin/export_cfg tgz"' > config.tgz*

**For Windows with PLINK.EXE**

*plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/export_cfg\"" > config.xml*

oder

*plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/export_cfg tgz\"" > config.tgz*

### 2.1.2 Upload configuration via SSH

**For Linux:**

a. a. Without router reboot:
   *cat config.xml | ssh admin@192.168.0.1 'su -c "/usr/sbin/store_cfg"'*
b. b. With subsequent router reboot:
   *cat config.xml | ssh admin@192.168.0.1 'su -c "/usr/sbin/store_cfg; /sbin/reboot"'*

The password is requested interactively by SSH. An automatic batch operation is not possible. You can, however, use the "sshpass" programme to run a script file comprising the password. The script file (for example, cfgupl.sh) must contain the following:

*#!/bin/bash cat config.xml | ssh admin@192.168.0.1 'su -c "/usr/sbin/store_cfg; /sbin/reboot"'*

The Linux command is as follows:

*sshpass -padmin ./cfgupl.sh*

**For Windows with PSCP.EXE and PLINK.EXE**

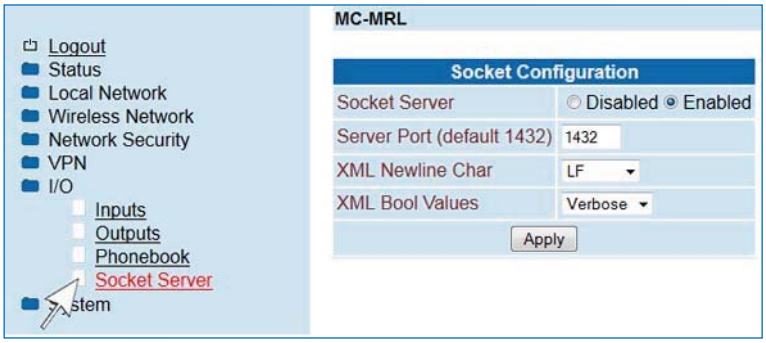
a. Without router-reboot:
   *pscp -scp -pw admin config.xml admin@192.168.0.1:/tmp/cfg.xml*
   *plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/store_cfg /tmp/cfg.xml\""*
b. With subsequent router reboot:
   *pscp -scp -pw admin config.xml admin@192.168.0.1:/tmp/cfg.xml*
   *plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/store_cfg /tmp/cfg.xml; /sbin/reboot\""*

## 2.2 Sending and receiving IO status, email, SMS and router status using XML files via the router socket server

The router includes an integrated socket server and can do the following by receiving XML files:

1. Set and query I/O signals
2. Send messages such as email and SMS
3. Query router status

To use these functions, the socket server must be set to "Enabled" as described under 1.8.4 (Page 34).
The socket server port can be freely configured, the default setting is port = 1432.



## 2.2.1 Sample for XML files

The following are a few examples of XML file content:

**Example: Setting and querying the I/O signals**

```
<?xml version="1.0"?>
<io>
<output no="1" value="1"/>
<input no="1"/>
</io>
```

**Example: Sending an email**

```
<?xml version="1.0"?>
<email to=name1@domain.de cc="name2@domain.de">
<subject>Test Mail</subject>
<body>Dies ist ein E-Mail-Text.
</body>
</email>
```

**Example: Sending an SMS**

```
<?xml version="1.0"?>
<cmgs destaddr="+49173 111223344">Dies ist der SMS-Text</cmgs>
```

**Example: Querying router status**

```
<?xml version="1.0"?>
<info>
<device />
<radio />
<ipsec />
<openvpn />
</info>
```

**Example: Activate the packet data connection (ab xmlsrvd-0.4.3)**

```
<?xml version="1.0"?>
<io>
<gprs value="1"/>
</io>
```

**Example: De-activate the packet data connection (ab xmlsrvd-0.4.3)**

```
<?xml version="1.0"?>
<io>
<gprs value="0"/>
</io>
```

**Example: Activate the IPsec connection n (Replace n with the IPsec tunnel number)**

```
<?xml version="1.0"?>
<io>
<ipsec no="n" value="1"/>
</io>
```

**Example: De-activate the IPsec connection n (Replace n with the IPsec tunnel number)**

```
<?xml version="1.0"?>
<io>
<ipsec no="n" value="0"/>
</io>
```

### 2.2.2 Functions test using Windows HyperTerminal

For a test in Windows, the programme "HyperTerminal" can be used. Hyperterminal can be used to send XML files to the router socket server. The corresponding (XML) files (see 2.2.1) must first be stored on your user PC.

Open Hyperterminal and configure the desired connection. (The example given uses the default settings):

**Host address:** 192.168.0.1 (Router / Socket Server IP-Address)

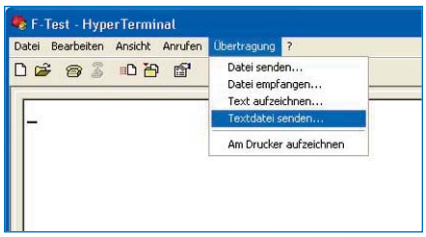
**Connection number:** 1432 (Socket Server Port)

**Establish connection via:** TCP/IP (Winsock)



Open the connection.

In the HyperTerminal menu "Transfer/send text file....", select the XML file to be transferred.




After transfer is complete, HyperTerminal displays the answer to your query.

## 2.3 Using the integrated GPS receiver in the MC-MRH router

This function is only available to you if you have an MC-MRH router with a GPS antenna connection.


The GPS coordinates (longitude and latitude) can be made available in different ways:

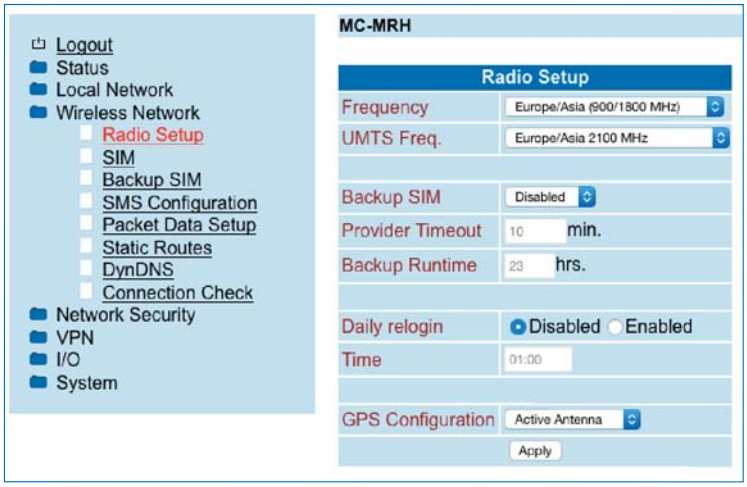
- In the web interface under "Status / Radio"
- By SMS as a reply to an SMS status request
- As a reply from the integrated socket server after receiving an XML file with status request

## 2.3.1 Activating the GPS function

Connect a passive or active GPS antenna to the "GPS" antenna terminal on the router. Please ensure that the GPS antenna has a "clear view" of the sky.

In the web interface, under "Wireless Network/Radio Setup" under "GPS Configuration" in the menu, select the type of antenna and click "Apply".

**Note:** If the setting "GPS configuration" is not visible, the GPS function is not activated for your router. If no antenna type is selected, no GPS data can be displayed.




## 2.3.2 Displaying the GPS coordinates in the web interface

Under "Status/Radio" in the menu, the data is displayed with the longitude and latitude values.


## 2.3.3 Receiving the GPS coordinates as an SMS

As described under 1.5.4 (SMS Configuration, Controlling the Cellular Router by SMS), a status notification can be requested by SMS.

#<password>:SEND:STATUS

Whten the GPS function is activated the GPS coordinates are transmitted in the SMS reply in addition to the status notification.

## 2.3.4 GPS coordinates as an XML file

As described under 2.2, the status of the router can be requested by sending an XML file to the socket server. When the GPS function is activated the GPS coordinates are transmitted in the status notification.